Attorney Docket No. 1083.1095

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Seigo KOTANI

Application No.: Group Art Unit:

Filed: October 31, 2003 Examiner:

For: SAFETY JUDGMENT METHOD, SAFETY JUDGMENT SYSTEM, SAFETY JUDGMENT APPARATUS, FIRST AUTHENTICATION APPARATUS, AND COMPUTER PROGRAM PRODUCT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-323200

Filed: November 6, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 31, 2003 By: _____

H. J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月　６日

出願番号
Application Number: 特願２００２－３２３２００

[ST. 10/C]: ［ＪＰ２００２－３２３２００］

出願人
Applicant(s): 富士通株式会社

２００３年　７月　９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５５４１９

【書類名】　特許願
【整理番号】　0295577
【提出日】　平成14年11月 6日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
G06F 17/60　222
【発明の名称】　安全性判断方法、安全性判断システム、安全性判断装置、第１認証装置及びコンピュータプログラム
【請求項の数】　20
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小谷　誠剛
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100078868
【弁理士】
【氏名又は名称】　河野　登夫
【電話番号】　06-6944-4141
【手数料の表示】
【予納台帳番号】　001889
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705356

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　安全性判断方法、安全性判断システム、安全性判断装置、第１認証装置及びコンピュータプログラム

【特許請求の範囲】

【請求項１】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、

予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、

前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

【請求項２】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法にお

いて、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第１認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記情報処理装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップと

を備えることを特徴とする安全性判断方法。

【請求項３】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェ

アの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を、前記第２認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、

予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、

前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第１認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

【請求項４】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から

取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

【請求項５】　前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第１認証装置へ送信するよう構成してあることを特徴とする請求項４に記載の安全性判断システム。

【請求項６】　前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、

前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付ける手段をさらに備え、

前記暗号化情報送信手段は、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第１認証装置へ送信するよう構成してあり、

前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、

前記第１認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送信する手段をさらに備えることを特徴とする請求項４に記載の安全性判断システム。

【請求項７】　前記第１認証装置は、

生体情報を受け付ける副生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、

前記第２認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第１認証装置を安全と判断する副安全判断手段と

を備えることを特徴とする請求項４に記載の安全性判断システム。

【請求項８】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフ

トウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記情報処理装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備える

ことを特徴とする安全性判断システム。

【請求項９】　前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給をうける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする請求項８に記載の安全性判断システム。

【請求項１０】　前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第２認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断するよう構成してあることを特徴とする請求項９に記載の安全性判断システム。

【請求項１１】　前記ソフトウェアは、前記情報処理装置に予めインストールされているソフトウェアのパッチ用ソフトウェアであることを特徴とする請求項８乃至１０に記載の安全性判断システム。

【請求項１２】　前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶された

データを消去する消去手段をさらに備えることを特徴とする請求項８乃至１０に記載の安全性判断システム。

【請求項１３】　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

前記第２認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

【請求項１４】　前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする請求項

４乃至１３のいずれかに記載の安全性判断システム。

【請求項１５】　前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする請求項４乃至１４のいずれかに記載の安全性判断システム。

【請求項１６】　第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段と、

前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第１認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断装置。

【請求項１７】　第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断

され、また前記環境情報送信手段により送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段と

を備えることを特徴とする安全性判断装置。

【請求項１８】　通信網を介して接続される情報処理装置の安全性を判断する第１認証装置において、

前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、

通信網を介して接続された第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理から送信された場合に、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、

前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする第１認証装置。

【請求項１９】　第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情

報送信ステップと、

コンピュータに、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信させる暗号化情報送信ステップと、

コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第１認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、前記第１認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップと

を実行させることを特徴とするコンピュータプログラム。

【請求項２０】　第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、

コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストールするインストールステップと

を実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法、安全性判断システム、安全性判断装置、第１認証装置及びコンピュータを安全性判断装置として機能させるためのコンピュータプログラムに関し、特に、携帯電話機、家電機器、パーソナルコンピュータ等の情報処理装置に組み込んで、該情報処理装置の安全性を判断する安全性判断装置等に関する。

【０００２】

【従来の技術】

ＩＰｖ６（Internet Protocol Version 6）の導入により、インターネット等の通信網に接続される情報処理装置は、パーソナルコンピュータ、サーバコンピュータ、及び携帯電話機だけではなく、冷蔵庫、電子レンジ、エアコン、ＴＶ、ＤＶＤ等の家電機器、コピー機、さらにはロボット等も通信網に接続され、情報の送受信が行われることになる。このように通信網に接続される情報処理装置が増加するにつれ、安全性（セキュリティ）が低下することになる。

【０００３】

特に家電機器は安全性が低く、外部から機器の正常な動作に支障をきたすプログラムを送り込まれるケースや、ＤＤｏＳ（Distributed Denial of Service）の踏み台にされる虞がある。そこで、このような情報処理装置の安全性を高めるために、指紋等を用いたバイオメトリック認証機能を情報処理装置に搭載する試みがなされている（例えば、引用文献１）。

【０００４】

【特許文献１】

特開平３－５８１７４号公報

【０００５】

【発明が解決しようとする課題】

しかしながら、認証用の指紋情報が流出する場合もあり、バイオメトリック認証のみでは、高度な安全性を確保することが難しいという問題があった。特にこ

れらの情報処理装置を用いた電子商取引を行う際には、情報処理装置が、正当な所有者が使用しているか、所有者自らの情報処理装置を用いた取引であるか、情報処理装置に安全性を損なう機器が接続、またはＯＳ(Operating System)、ブラウザ、プラグインソフト等のソフトウェアがインストールされていないか等の安全性をまず確保した上で、商取引を行うことが好ましい。

【０００６】

また、これらの情報処理装置にパッチ用のソフトウェア、ファームウェア等を提供する場合、第３者に送信中のソフトウェアを改竄される虞があることから、情報送信側の装置と情報処理装置との間での安全性を十分に確保する必要があった。その一方で、安全性のレベルを高めすぎると、円滑な情報の送受信を行うことが困難となる。

【０００７】

本発明は斯かる事情に鑑みてなされたものであり、その目的とするところは、生体情報を用いた認証、認証機関を利用した電子証明書による認証（ＰＫＩ(Public Key Infrastructure認証)、及び情報処理装置の利用環境の階級を利用した環境情報を用いた認証を組み合わせて認証を行うことにより、安全性を高めることができ、また妥当な安全性を維持した上で円滑に情報の送受信を行うことが可能な安全性判断方法、安全性判断システム、安全性判断装置、第１認証装置及びコンピュータを安全性判断装置として機能させるためのコンピュータプログラムを提供することにある。

【０００８】

また、本発明の他の目的は、商取引が行われる商品の価値に応じて安全性の階級を変化させることにより、安全性を確保した上で円滑な商取引を実現することが可能な安全性判断システムを提供することにある。

【０００９】

さらに、本発明の他の目的は、主電力供給手段とは別の副電力供給手段からの電力供給をうける受信用通信手段をもちいて、パッチ用ソフトウェア等を受信して蓄積しておくことにより、安全性を確保した上で容易にパッチ用ソフトウェア等を配布することが可能な安全性判断システムを提供することにある。

【００１０】

【課題を解決するための手段】

第１発明に係る安全性判断方法は、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップとを備えることを特徴とする。

【００１１】

第２発明に係る安全性判断方法は、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報

を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第１認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、前記情報処理装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップとを備えることを特徴とする。

【００１２】

第３発明に係る安全性判断方法は、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報を、前記第２認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第１認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、前

記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップとを備えることを特徴とする。

【００１３】

第４発明に係る安全性判断システムは、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、前記第１認証装置は、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

【００１４】

第５発明に係る安全性判断システムは、第４発明において、前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第１認証装置へ送信するよう構成してあることを特徴とする。

【００１５】

第６発明に係る安全性判断システムは、第４発明において、前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付け

る手段をさらに備え、前記暗号化情報送信手段は、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第１認証装置へ送信するよう構成してあり、前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、前記第１認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送信する手段をさらに備えることを特徴とする。

【００１６】

第７発明に係る安全性判断システムは、第４発明において、前記第１認証装置は、生体情報を受け付ける副生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、前記第２認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、前記第２認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、前記情報処理装置は、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第１認証装置を安全と判断する副安全判断手段とを備えることを特徴とする。

【００１７】

第８発明に係る安全性判断システムは、情報処理装置、第１認証装置及び第２

認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第１認証装置へ送信する環境情報送信手段とを備え、前記第１認証装置は、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記情報処理装置は、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備えることを特徴とする。

【００１８】

第９発明に係る安全性判断システムは、第８発明において、前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給をうける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする。

【００１９】

第１０発明に係る安全性判断システムは、第９発明において、前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第２認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断す

るよう構成してあることを特徴とする。

【００２０】

第１１発明に係る安全性判断システムは、第８発明乃至第１０発明のいずれかにおいて、前記ソフトウェアは、前記情報処理装置に予めインストールされているソフトウェアのパッチ用ソフトウェアであることを特徴とする。

【００２１】

第１２発明に係る安全性判断システムは、第８発明乃至第１０発明のいずれかにおいて、前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶されたデータを消去する消去手段をさらに備えることを特徴とする。

【００２２】

第１３発明に係る安全性判断システムは、情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、前記第２認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、前記第２認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、前記第１認証装置は、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段とを備える

ことを特徴とする。

【００２３】

第１４発明に係る安全性判断システムは、第４発明乃至第１３発明のいずれかにおいて、前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする。

【００２４】

第１５発明に係る安全性判断システムは、第４発明乃至第１４発明のいずれかにおいて、前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする。

【００２５】

第１６発明に係る安全性判断装置は、第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段と、前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第１認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

【００２６】

第１７発明に係る安全性判断装置は、第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報

を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断され、また前記環境情報送信手段により送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段とを備えることを特徴とする。

【００２７】

第１８発明に係る第１認証装置は、通信網を介して接続される情報処理装置の安全性を判断する第１認証装置において、前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、通信網を介して接続された第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理から送信された場合に、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

【００２８】

第１９発明に係るコンピュータプログラムは、第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュー

タプログラムにおいて、コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情報送信ステップと、コンピュータに、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信させる暗号化情報送信ステップと、コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第１認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、前記第１認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップとを実行させることを特徴とする。

【００２９】

第２０発明に係るコンピュータプログラムは、第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情報送信ステップと、コンピュータに、前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストールするインストールステップとを実行させることを特

徴とする。

【００３０】

本発明にあっては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かを判断する。また、情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する。具体的には、情報処理装置自身の機器名、バージョン、情報処理装置に接続されている機器の名称、インストールされているブラウザ名、ＯＳ名、バージョン等の情報が該当する。情報処理装置は収集した環境情報を第１認証装置へ送信する。

【００３１】

さらに、第３者的な立場にある認証機関等の第２認証装置から発行を受けた電子証明書及び情報処理装置の個人鍵で暗号化された商取引に関する情報等を第１認証装置へ送信する。第１認証装置は、電子証明書及び暗号化された情報を受信した場合、第２認証装置から取得した第２認証装置（認証機関）の公開鍵を用いて、送信された電子証明書から情報処理装置の公開鍵を取得する。そして、取得した情報処理装置の公開鍵で暗号化された情報を復号し、復号された情報が適正であるか否かをメッセージダイジェストなどを用いて判断する。

【００３２】

第１認証装置は、送受信される情報に応じて階級付けされた環境情報の条件を記憶した環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。つまり、送受信される情報に対して高度な安全性を確保する必要がある場合、情報処理装置の環境情報は、より条件の厳しい（階級の高い）環境条件を満たす必要がある。例えば、高度な安全性が必要とされる場合（例えば、株取引、５万円以上の高額商品の取引）は、情報処理装置のＯＳが最新のバージョンであることを条件としておき、情報処理装置のＯＳが最新のバージョンである場合は、環境認証が適正であると判断し、情報処理装置のＯＳが最新のバージョンでない場合（旧バージョンのＯＳの場合など）は、セキュリティホールがある虞があるので、環境認証が適正でないと判断する。

【００３３】

一方、低価格商品の取引の場合、安全性よりも利便性を確保する必要があるの

で、高い階級の条件を満たす必要はなく、多少セキュリティホールのあるバージョンの古いＯＳをインストールしている場合でも環境認証が適正であると判断させる。例えば、１００円程度の、商品の取引の場合は、情報処理装置のＯＳが旧バージョンであったとしても環境認証が適正であると判断する。そして、生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置を安全と判断する、例えば安全であることを示すフラグをセットし、安全であることを示す情報を、商取引を行う店舗コンピュータへ通知し、安全性を確保した上で情報処理装置と店舗コンピュータとの間の、情報の送受信を行う。このように構成したので、情報処理装置の安全性を確保しつつ、円滑な情報の送受信及び商取引を実現することが可能となる。さらに、第１認証装置においても生体情報認証、電子証明書認証及び環境認証をおこない、情報処理装置における生体情報認証、電子証明書認証及び環境認証、並びに、第１に認証装置における生体情報認証、電子証明書認証及び環境認証において、全て適正と判断された場合のみ、第１認証装置及び情報処理装置の双方を安全と判断するようにしたので、さらに高度な安全性を確保することが可能となる。

【００３４】

また、本発明にあっては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かの本人認証を行う。そして上述したように情報処理装置は収集した環境情報を第１認証装置へ送信し、第１認証装置において、環境情報の認証を行う。第１認証装置から情報処理装置へパッチ用のソフトウェア等を送信する場合は、第１認証装置は、第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを情報処理装置へ送信する。

【００３５】

前記情報処理装置は、電子証明書及び暗号化されたソフトウェアを受信した場合、第２認証装置へ公開鍵を要求し、この認証機関の公開鍵を用いて電子証明書から第１認証装置の公開鍵を取得する。そしてこの公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。最後に、上述した本人認証、環境認証及び電子証明書による認証が全て適正であると判断した場合、復号したソフトウェアを情報処理装置へインストールする。この

ように構成したので、第３者のなりすましを防止でき、高度な安全性を維持した上で情報処理装置へパッチ用のソフトウェア、ファームウェア等のソフトウェアを提供することが可能となる。

【００３６】

さらに、本発明にあっては、情報処理装置は、主電力供給手段及び副電力供給手段を備え、受信用通信手段は副電力供給手段から電力の供給をうける構成としている。主電力供給手段による電力の供給が行われていない場合、すなわちメインの電源がオンにされていない場合に、第１認証装置から電子証明書及び個人鍵で暗号化されたソフトウェアが送信された場合は、サブバッテリーを用いた受信用通信手段によりこれらの情報を受信して蓄積する。そして、主電力供給手段による電力の供給が行われた場合に、蓄積した電子証明書及びソフトウェアを読み出し、送信されたソフトウェアが適正であるか否かの判断、本人認証及び環境認証を行うようにしたので、電源をオンにしていない顧客に対してもパッチ用のソフトウェアを、安全性を確保した上で大量に配布することが可能となる。また特に提供するソフトウェアとして、所定の日時以降に記憶されたデータを記憶部から消去するソフトウェアを提供することによりＤＤｏＳ攻撃の踏み台にされることを効果的に防止することが可能となる。

【００３７】

【発明の実施の形態】

以下本発明を実施の形態を示す図面に基づいて詳述する。

実施の形態１

実施の形態１では、情報処理装置を携帯電話機であるものとし、本発明に係る安全性判断システムを、携帯電話機を用いた商取引に適用した場合について説明する。なお、情報処理装置は携帯電話機に限定されるものではなく、パーソナルコンピュータ、コピー機、プリンタ、ＦＡＸ、冷蔵庫、ＴＶ、ＤＶＤプレーヤ、ＰＤＡ(Personal digital Assistant)、空気調和機、電子レンジ、ロボット等であっても良い。

【００３８】

図１は本発明に係る安全性判断システムの概要を示す模式図である。図におい

て１は情報処理装置としての携帯電話機、３は電子証明書の発行を行う第３者的立場にある認証機関の第２認証装置（以下、認証機関サーバという）、２は安全性判断局であって携帯電話機１の安全性を判断する第１認証装置としての中央サーバ、４はオンラインでの商品の販売処理を行うオンラインショップの店舗コンピュータ（以下、Ｗｅｂサーバという）である。携帯電話機１は図示しない携帯電話網を介して、通信網（以下、インターネットという）Ｎに接続されており、同様に認証機関サーバ３、中央サーバ２、及びＷｅｂサーバ４もインターネットＮに接続されている。携帯電話機１には生体情報受付手段として指紋取得部１１２が設けられており、顧客の指紋をスキャンして携帯電話機１に取り込む機能を有する。

【００３９】

図２は携帯電話機１のハードウェア構成を示すブロック図である。情報処理装置としての携帯電話機１は通話、文字、画像データの送受信等、通常の機能を果たす携帯電話機エンジン部１１０及び本発明に係る安全性判断装置５から構成される。本実施の形態においては、安全性判断装置（以下、セキュリティチップという）５はＬＳＩ（Large Scale Integrated Circuit）チップであり、携帯電話機１の内部に実装される。

【００４０】

以下に、携帯電話機エンジン部１１０のハードウェア構成について説明する。図に示すように、ＣＰＵ(Central Processing Unit)１１にはバス１７を介してＲＡＭ１２，ＲＯＭ１５、アンテナ部１６、電源部１１３、マイク・スピーカ１１１、ＡＤ／ＤＡ１１２，外部接続端子１９，データ表示用の液晶ディスプレイ等の表示部１４、及び数字キー、カーソルキー、選択確定キー等から構成される入力部１３等が接続される。ＣＰＵ１１は、バス１７を介して携帯電話機１の上述したようなハードウェア各部と接続されていて、それらを制御すると共に、ＲＯＭ１５に格納された制御プログラム１５Ｐに従って、種々のソフトウェア的機能を実行する。

【００４１】

外部接続端子１９は例えば１６芯からなるインターフェースであり、ＵＳＢケ

ーブル等を介して、図示しないパーソナルコンピュータ、または周辺機器と接続される。ＲＡＭ１２は、ＳＲＡＭ(Static Random Access Memory)またはフラッシュメモリ等で構成され、ソフトウェアの実行時に発生する一時的なデータを記憶する。ＲＯＭ１５は例えばＥＥＰＲＯＭ(Electrically Erasable and Programmable ROM)等で構成され、携帯電話機１の基本的操作環境を提供するＯＳ(Operating System)、外部接続端子１９に接続された周辺機器等を制御するＢＩＯＳ(Basic Input/Output System)、及びダウンロードまたは予めインストールされているＪａｖａ（登録商標）等のソフトウェアが記憶されている。

【００４２】

携帯電話機エンジン部１１０の入力部１３とは別に、顧客の指紋を取得する指紋取得部１１２が携帯電話機１の入力部１３の近傍に設けられている。指紋取得部１１２はスキャンして読み取った指紋データをセキュリティチップ５へ出力する。なお、本実施の形態においては生体情報として指紋を用いることとしたが、これに限るものではなく、音声、網膜、または虹彩等の情報であっても良い。例えば、音声の場合マイク・スピーカ１１１から音声を取得し、音声をＡＤ／ＤＡ１１２を用いて電気信号に変換し、ＣＰＵ１１へ出力し、予め記憶してある顧客本人の音声データと比較することにより認証を行う。

【００４３】

次に、セキュリティチップ５のハードウェア構成について説明する。セキュリティチップ５は、マイクロプロセッサ（以下、ＭＰＵという）５１、ＲＡＭ５２、ＥＥＰＲＯＭ等のＲＯＭ５５を備えている。ＭＰＵ５１は、バス５７を介して上述したＲＡＭ５２及びＲＯＭ５５と接続されていて、それらを制御すると共に、ＲＯＭ５５に格納された制御プログラム５５Ｐに従って、種々のソフトウェア的機能を実行する。ＲＯＭ５５には、認証機関サーバ３から受信した電子証明書を記憶する電子証明書ファイル５５３、携帯電話機１自身の個人鍵を記憶する個人鍵ファイル５５４、予め顧客の指紋情報を記憶した指紋情報ファイル５５２、及び、携帯電話機１の機器名・バージョン、周辺機器の機器名・バージョン、インストールされているソフトウェアのソフト名・バージョン等を記憶した環境情報ファイル５５１が用意されている。なお、携帯電話機１の個人鍵は認証機関サ

ーバ３により発行され、この個人鍵と対になる携帯電話機１の公開鍵は任所機関サーバ３が管理している。

【００４４】

セキュリティチップのＭＰＵ５１は携帯電話機１の環境情報を収集して環境情報ファイル５５１に環境情報を記憶する。ＭＰＵ５１は、予め記憶されている携帯電話機１の機器名・バージョンをＲＯＭ１５１から取得し、携帯電話機１自身の情報を取得する。例えば、情報処理装置が携帯電話機である場合、機器名・バージョン、情報処理装置が電子レンジである場合、メーカー名、機器名、型番等を取得する。また、ＭＰＵ５１は、ＲＯＭ１７のＢＩＯＳを参照して、外部接続端子１９に接続された機器の情報を取得して環境情報の一つとして環境情報ファイル５５１に記憶する。例えば、図示しないコンピュータが外部接続端子１９に接続された場合、コンピュータの機器名等が取得される。また情報処理装置がパーソナルコンピュータである場合に、外部接続端子１９としてのＰＣカードスロットにＰＣカードが接続された場合は、該ＰＣカードの機器名等を取得する。

【００４５】

環境情報としてはさらに、携帯電話機１にインストールされているソフトウェアの情報が該当する。ＭＰＵ５１はＲＯＭ１５のＯＳ及びソフトウェアを参照し、インストールされているソフトウェアの名称及びバージョンを取得する。例えば、情報処理装置がパーソナルコンピュータである場合、ＯＳの名称としてウィンドウズ（登録商標）またはＬｉｎｕｘ、バージョンとしてSecond Edition等の環境情報が取得され、インストールされているソフトウェアとしてブラウザのインターネットエクスプローラ（登録商標）、バージョンとしてＳＰ２等の情報が取得される。その他、インターネットＮを通じてダウンロードしたＪａｖａ（登録商標）等で記述されたソフトウェアの名称などが該当する。このようにＭＰＵ５１はＲＯＭ内のＢＩＯＳ、ＯＳ等を常時監視しており、新たなソフトウェアがインストールされた場合、または外部接続端子１９に新たな機器が接続された場合、環境情報としてそれらの情報を収集して環境情報ファイル５５１に記憶する。

【００４６】

指紋情報ファイル５５２は本人認証のために用いるものであり、例えば携帯電話機１の購入時に、店舗において顧客の指紋を取得しＲＯＭ５５内の指紋情報ファイル５５２に初期登録する。ＭＰＵ５１は指紋取得部１１２から、指紋情報が読み取られて出力された場合は、出力された指紋情報と指紋情報ファイル５５２に記憶した指紋情報とを比較して適正か否かを判断する。なお、本実施の形態においては認証に用いる指紋情報ファイル５５２を携帯電話機１に設けることとしているが、これに限るものではなく、中央サーバ２または認証機関サーバ３等に設け、中央サーバ２または認証機関サーバ３等で、認証を行うようにしても良い。この場合、個人鍵ファイル５５４の個人鍵で暗号化された指紋情報が電子証明書と共に中央サーバ２または認証機関サーバ３へ送信され認証が行われる。

【００４７】

電子証明書ファイル５５３には認証機関サーバ３から発行を受けた電子証明書が記憶されており、また個人鍵ファイル５５４には同じく認証機関サーバ３から発行を受けた携帯電話機１用の個人鍵が記憶されている。なお、携帯電話機１用の公開鍵は認証機関サーバ３が記憶している。ＭＰＵ５１は送受信される商取引に関するデータ、また環境情報、指紋情報等については、メッセージダイジェスト共に個人鍵で暗号化し、暗号化データと電子証明書とをインターネットＮを介して中央サーバ２等に送信する。

【００４８】

図３は中央サーバ２のハードウェア構成を示すブロック図である。図に示すように、ＣＰＵ(Central Processing Unit)２１にはバス２７を介してＲＡＭ２２，ハードディスク等の記憶部２５、携帯電話機１、認証機関サーバ３及びＷｅｂサーバ４等と情報を送受信するためのゲートウェイ、ＬＡＮカード等の通信部２６，液晶ディスプレイ等の表示部２４、及びキーボード、マウス等の入力部２３が接続される。ＣＰＵ２１は、バス２７を介して中央サーバ２の上述したようなハードウェア各部と接続されていて、それらを制御すると共に、記憶部２５に格納された制御プログラム２５Ｐに従って、種々のソフトウェア的機能を実行する。また、記憶部２５には送受信される情報の安全性の階級に応じて環境条件が記憶された環境情報データベース（以下、環境情報ＤＢという）２５１が設けられ

ている。

【００４９】

図４は環境情報ＤＢ２５１のレコードレイアウトを示す説明図である。図に示すように階級に応じて環境情報の条件が記憶されている。階級フィールドは送受信される情報の安全性の重要度に応じて１～６に階級付けされており、階級１が最も安全性のレベルが高く、階級６が安全性のレベルが最も低いことを示す。金額情報フィールド及び商品情報フィールドに示すように、１００円程度の少額の取引、または商品が着信メロディ（以下、着メロという）等の価格の低い商品等の場合は、安全性よりも円滑な取引を重視する必要があることから、階級が６とされている。一方、５００００円以上の高額商品の取引である場合、商品が株券等の場合は、高い安全性を確保する必要があるので階級が１とされている。

【００５０】

環境条件フィールド中の装置情報フィールドには顧客の携帯電話機１の機器名・バージョンが階級に対応づけられて記憶されている。例えば、階級１の場合、最新機種であるＳ００４，Ｆ００４，及びＮ００４である携帯電話機１であることが条件とされており、環境情報としてこの条件を満たさない限り環境認証において適正と判断されない。特にＳ００４については、携帯電話機１のバージョンが２．０以上であることも条件とされている。これに対し、階級６の場合、古い機種であるＳ００１を含め、Ｓ００１，Ｓ００２，Ｓ００３及びＳ００４の他、同様にＦ００１～Ｆ００４、並びにＮ００１～Ｎ００４の携帯電話機１であれば、適正と判断される。

【００５１】

周辺機器フィールドも同様に階級毎に周辺機器の機器名及びバージョンが記憶されており、環境認証に利用される。例えば、階級６の場合は、周辺機器ＸＸ，ＸＹ等が接続されている場合でも、環境認証において適正と判断される。その一方で階級１の場合は、対応する周辺機器の条件が記憶されておらず、環境情報として携帯電話機１から、周辺機器の情報が送信された場合は、適正と判断されない。すなわち階級１の場合はいかなる周辺機器が接続されていても環境認証において不適正と判断される。なお、これらの情報は各ベンダーから提供されるもの

を記憶している。

【００５２】

同じくソフトウェアフィールドも階級に応じてソフトウェア名及びバージョンが記憶されている。階級６ではソフトウェアＣであって、バージョンが３．０以上の場合に適正と判断される。その一方で、階級６の場合はソフトウェアＣであってバージョンが１．０以上であれば適正と判断される。このように階級を設けて安全性を判断したのは、円滑な商取引と安全性の維持とのバランスを考慮したものである。例えば、情報処理装置がパーソナルコンピュータである場合、インストールされるブラウザは顧客によって異なる。例えば、マイクロソフト（登録商標）社のインターネットエクスプローラ（登録商標）では、複数のバージョンが存在し、バージョンが上がるに連れセキュリティホールの存在が少なくなっている。

【００５３】

高度な安全性が要求される場合は、環境情報を取得して、セキュリティホールのない最新のバージョンのブラウザである場合にのみ適正であると判断し、以降の商取引を許可することも考えられるが、そうすると、最新のバージョンをインストールしていない顧客は全く商取引を行うことができず妥当性を欠くことになる。そこで、安全性がそれほど要求されない低額商品等である場合は、認証の階級を低くし、多少バージョン古いブラウザであっても、一定条件下で適正と判断し商取引を認めることとしたものである。

【００５４】

以上のハードウェア構成において本発明における安全性判断の処理手順を、フローチャートを用いて説明する。図５はＷｅｂサーバ４と携帯電話機１との間の商取引の手順を示すフローチャートである。まず、携帯電話機１の入力部１３に商取引を行うオンラインショップのＷｅｂサーバ４のＵＲＬ(Uniform Resource Locater)を入力して、商品発注ページの取得要求をＷｅｂサーバ４に対して行う（ステップＳ５１）。ＨＴＴＰ（Hypertext Transfer Protocol）サーバとしてのＷｅｂサーバ４は図示しない記憶部から対応するｃＨＴＭＬ(compact Hypertext Markup Language)ファイルを読み出し（ステップＳ５２）、読み出したｃＨ

ＴＭＬファイルを携帯電話機１へ送信する（ステップＳ５３）。

【００５５】

携帯電話機１のＣＰＵ１１は受信したｃＨＴＭＬをＲＯＭ１５に記憶したブラウザソフトウェアにて解析し、図６の如く商取引のＷｅｂページを表示する（ステップＳ５４）。図６はＷｅｂページのイメージを示す説明図である。図に示すように表示部１４には発注する商品、数量、及び金額の情報が表示される。顧客は発注する商品及び数量を、入力部１３を操作して選択する。商品が選択された場合は、ＣＰＵ１１はｃＨＴＭＬファイルと同時に送信されたＪａｖａスクリプトを実行し合計金額を算出して表示する。本実施の形態におけるオンラインショップは、パーソナルコンピュータ、プリンタ、ディスクドライブ等のコンピュータ関連機器を販売しており、顧客は２９８００円のインクジェットプリンタを１台注文する様子を示している。すなわち顧客は商取引に関する注文情報として、金額情報または商品情報を入力する。この他、住所、電話番号、氏名、ＩＤ、パスワード等を入力させるようにしても良い。

【００５６】

このようにして入力部１３から注文情報が入力され、ＣＰＵ１１はこの注文情報を受け付ける（ステップＳ５５）。そして、図６に示す「発注する」ボタンが選択された場合、安全性の判断処理に移行する（ステップＳ５６）。なお、ステップＳ５７以降の処理については後述する。以下に、本発明の特徴である安全性の判断処理のサブルーチンを、フローチャートを用いて説明する。

【００５７】

図７乃至図１２は安全性の判断処理の手順を示すフローチャートである。注文情報が入力された場合、セキュリティチップ５のＭＰＵ５１は制御プログラム５５Ｐを実行し、表示部１４に指紋情報の取得要求を表示する（ステップＳ７１）。表示する内容は予めＲＯＭ５５に記憶されており、「例えば、指紋取得部に親指をおいて下さい。」等の情報を読み出して表示部１４へ出力するようにすればよい。指紋取得部１１２から指紋情報が入力された場合、セキュリティチップ５のＭＰＵ５１は指紋情報を受け付け（ステップＳ７２）、ＲＡＭ５２に一時的に記憶する。そして、ＭＰＵ５１はＲＯＭ５５の指紋情報ファイル５５２に携帯電

話機１の購入時に予め記憶してある指紋情報を読み出し、ＲＡＭ５２に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップＳ７３）。

【００５８】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップＳ７３でＹＥＳ）、指紋認証適正フラグをセットし、セットした指紋認証適正フラグを中央サーバ２へ送信する（ステップＳ７５）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップＳ７３でＮＯ）、指紋認証不適正フラグセットし、セットした指紋認証不適正フラグを中央サーバ２へ送信する（ステップＳ７４）。中央サーバ２のＣＰＵ２１は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部２５に記憶する（ステップＳ７７）。なお、本実施の形態においては指紋を用いた生体認証を携帯電話機１において実行することとしたが、予め採取した指紋情報を認証機関サーバ３または中央サーバ２に記憶しておき、認証機関サーバ３または中央サーバ２において判断するようにしても良い。これにより指紋を用いた生体認証が終了する。

【００５９】

続いて、電子証明書を用いた認証へ移行する。セキュリティチップ５のＭＰＵ５１は、ステップＳ５５で入力された注文情報に、ＲＯＭ５５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ７６）。ＭＰＵ５１は認証機関サーバ３から予め発行を受けた携帯電話機１の個人鍵を個人鍵ファイル５５４から読み出し、注文情報及びメッセージダイジェストを暗号化する（ステップＳ８１）。さらに、ＭＰＵ５１は電子証明書ファイル５５３から認証機関サーバ３において予め発行を受けた電子証明書を読み出し、暗号化した注文情報及びメッセージダイジェストに電子証明書を添付して中央サーバ２へ送信する（ステップＳ８２）。中央サーバ２のＣＰＵ２１は送信された電子証明書、暗号化された注文情報及びメッセージダイジェストをＲＡＭ２２に記憶する。

【００６０】

中央サーバ２のＣＰＵ２１は電子証明書に記載されている認証機関サーバ３へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求す

る（ステップＳ８３）。認証機関サーバ３は、電子証明書の公開鍵を中央サーバへ送信する（ステップＳ８４）。中央サーバ２のＣＰＵ２１は、記憶した電子証明書をＲＡＭ２２から読み出し、認証機関サーバ３から送信された認証機関の公開鍵を用いて電子証明書を復号し、携帯電話機１の公開鍵を取得する（ステップＳ８５）。

【００６１】

中央サーバ２のＣＰＵ２１は取得した携帯電話機１の公開鍵を用いて暗号化された注文情報及びメッセージダイジェストを復号する（ステップＳ９１）。さらにＣＰＵ２１は復号した注文情報に、中央サーバ２の記憶部２５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ９２）。中央サーバ２のＣＰＵ２１はステップＳ９１で復号したメッセージダイジェストと、ステップＳ９２で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある顧客の携帯電話機１から情報が送受信されたものであるか否かを判断する（ステップＳ９３）。

【００６２】

メッセージダイジェストが一致しない場合は（ステップＳ９３でＮＯ）、ＣＰＵ２１は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップＳ９５）。一方、メッセージダイジェストが一致する場合は（ステップＳ９３でＹＥＳ）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップＳ９４）。そして、中央サーバ２のＣＰＵ２１は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）を記憶部２５に記憶する（ステップＳ９６）。これにより、電子証明書を用いた認証が終了する。

【００６３】

続いて環境認証について説明する。セキュリティチップ５のＭＰＵ５１は携帯電話機１の環境情報を取得する（ステップＳ１０１）。環境情報の収集は、上述したようにＭＰＵ５１が携帯電話機１のＲＯＭ１５のＯＳ、ＢＩＯＳ及びインストールされるソフトウェアを常駐して監視し、携帯電話機１の機器名、ＯＳの名称、バージョン、外部接続端子１９に接続された周辺機器の機器名、バージョン

、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル５５１に記憶される（ステップＳ１０２）。

【００６４】

ＭＰＵ５１は環境情報ファイル５５１から収集した環境情報を読み出して中央サーバ２へ送信する（ステップＳ１０３）。中央サーバ２のＣＰＵ２１は送信された環境情報をＲＡＭ２２に記憶する。中央サーバ２のＣＰＵ２１はステップＳ９１にて復号した注文情報に対応する階級の読み出しを、環境情報ファイル２５１を参照して行う（ステップＳ１０４）。つまり、ＣＰＵ２１は金額情報または商品情報フィールドを参照して、注文情報中の取り引きされる金額または商品等を基に、対応する階級を階級フィールドから読み出す。例えば注文する商品の金額が５００００円を超える場合は階級１が選択される。

【００６５】

ＣＰＵ２１は読み出した階級に対応する環境情報の条件を環境情報ＤＢ２５１から読み出す（ステップＳ１０５）。つまり、読み出した階級を基に、環境条件フィールドから対応する携帯電話機１の装置名・バージョン、ソフト名・バージョン、周辺機器の機器名・バージョンを読み出す。そして、ＣＰＵ２１は、ＲＡＭ２２に記憶され、受信した環境情報が、読み出した環境情報の条件を満たすか否かを判断する（ステップＳ１１１）。条件を満たさない場合（ステップＳ１１１でＮＯ）（例えば階級が１であり、環境情報としてソフトウェアＣのバージョン２．０が送信された場合、バージョン３．０以上という条件を満たさない）、環境認証不適正フラグをセットする（ステップＳ１１２）。一方、条件を満たす場合（ステップＳ１１１でＹＥＳ）、環境認証適正フラグをセットする（ステップＳ１１３）。例えば、条件として階級が１の場合に、環境情報として「携帯電話機１の装置名が最新機種Ｆ００４、バージョンは２．０、ソフトウェアはソフトウェアＣのバージョン５．０がインストールされており、かつ周辺機器に何も接続されていない」場合、環境が適正であると判断する。中央サーバ２のＣＰＵ２１は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部２５に記憶する（ステップＳ１１４）。これにより環境認証が終了する

。

【００６６】

ＣＰＵ２１は、記憶部２５に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップＳ１１５）。全ての適正フラグがセットされている場合（ステップＳ１１５でＹＥＳ）、携帯電話機１を安全なものと判断し安全フラグをセットする（ステップＳ１２１）。換言すれば、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の全てにおいて適正と判断された場合に限り携帯電話機１を適正なものであると判断する。中央サーバ２のＣＰＵ２１は安全であることを示す安全保証情報及び注文情報をＷｅｂサーバ４へ送信する（ステップＳ１２２）。

【００６７】

一方、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の内、１つでも不適正フラグがセットされている場合は、不適正フラグをセットする（ステップＳ１２３）。この場合ＣＰＵ２１は携帯電話機１が危険であることを示す危険情報をＷｅｂサーバ４へ送信し（ステップＳ１２４）、安全性判断のサブルーチン（ステップＳ５６）を終了する。

【００６８】

図５において、Ｗｅｂサーバ４は、携帯電話機１の危険情報を中央サーバ２から受信したか否かを判断する（ステップＳ５７）。危険情報を受信していない場合（ステップＳ５７でＮＯ）、Ｗｅｂサーバ４は安全保証情報及び注文情報を受信したか否かを判断する（ステップＳ５８）。安全保証情報及び注文情報を受信していない場合（ステップＳ５８でＮＯ）、またステップＳ５７においてＹＥＳの場合、携帯電話機１は不正の可能性が高いとして、商取引の中止を求める情報を携帯電話機１へ送信する（ステップＳ５９）。一方、安全保証情報及び注文情報を受信した場合（ステップＳ５８でＹＥＳ）、携帯電話機１の安全性は保証されたものであるものとして、注文の受注を正式に行い、受注を行われたことを示す受注確認情報を携帯電話機１へ送信する（ステップＳ５１０）。このように、商取引に先立ち、本人認証、ＰＫＩ認証及び環境認証を行って十分な安全性を確

保すると共に、取り引きされる商品の価値に応じて認証レベルを変化させることで円滑な商取引を実現することが可能となる。

【００６９】

実施の形態２

図１３は実施の形態２に係る携帯電話機１のハードウェア構成を示すブロック図である。実施の形態１に係る携帯電話機１を実行させるためのコンピュータプログラムは、本実施の形態２のように携帯電話機１にプレインストールして提供することも、またＣＤ－ＲＯＭ、ＭＯ、メモリーカード等の可搬型記録媒体で提供することも可能である。さらに、コンピュータプログラムを回線経由で搬送波として伝搬させて提供することも可能である。すなわち、セキュリティチップ５を搭載する代わりに、セキュリティチップ５と同様の機能をもつコンピュータプログラムを携帯電話機１のＲＯＭ１５にインストールするようにしても良い。以下に、その内容を説明する。

【００７０】

図１３に示す携帯電話機１に、生体情報を認証させ、環境情報を収集させ、環境情報を送信させ、暗号化情報を送信させ、安全性を判断させるプログラムが記録された記録媒体１ａ（ＣＤ－ＲＯＭ、ＭＯ、メモリーカード又はＤＶＤ－ＲＯＭ等）が携帯電話機１のＲＯＭ１５にインストールされている。インストールの方法としては、外部接続端子１９に接続可能なメモリーカード等の記録媒体１ａを嵌挿し、プログラムをインストールするか、または、中央サーバ２から本発明に係るプログラムをダウンロードする。係るプログラムは携帯電話機１のＲＡＭ１２にロードして実行される。これにより、上述のような本発明の情報処理装置としての携帯電話機１として機能する。

【００７１】

実施の形態３

実施の形態１においては、生体情報の認証をセキュリティチップ５において行うこととしたが、中央サーバ２または認証機関サーバ３において実行しても良い。実施の形態２は、生体情報の認証を中央サーバ２において実行する形態であって、また予めセキュリティポリシーが決定されている場合に、本発明を適用した

形態について説明する。

【００７２】

図１４は実施の形態３に係る携帯電話機１のハードウェア構成を示すブロック図であり、図１５は中央サーバ２のハードウェア構成を示すブロック図である。図１４及び図１５に示すように生体情報の認証は中央サーバ２で実行するため、認証用の指紋情報ファイル２５２は携帯電話機１の内部ではなく中央サーバ２の記憶部２５に記憶されている。なお、認証用の指紋情報は、認証前に、顧客に店舗、サービスセンター等に来店してもらい、免許証、パスポートなどで本人であることを確認した上で、その場で指紋を読み取るなどして初期登録するようにすればよい。

【００７３】

図１６乃至図２０は実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。まず、セキュリティチップ５のＭＰＵ５１は以後の通信を行うために、安全性の確認を開始することを示す信号を中央サーバ２へ送信する（ステップＳ１６１）。中央サーバ２のＣＰＵ２１は確認開始信号を受信した場合、通信の安全性の階級を決定する（ステップＳ１６２）。この階級の決定にあたっては、予め決定したセキュリティポリシーに従って決定する。例えば、以後行われる通信が、住民票の発行、株取引等、高い安全性が必要とされる場合は階級１と決定され、着メロ、待ち受け画面の画像データ等、安全性がそれほど要求されない場合は、階級６とされる。また公共料金の支払い等においては、中程度の安全性を確保するために階級３と決定する。

【００７４】

中央サーバ２のＣＰＵ２１は階級の決定後、確認開始信号に対する応答信号を携帯電話機１へ送信する（ステップＳ１６３）。応答信号を受信した場合、セキュリティチップ５のＭＰＵ５１は制御プログラム５５Ｐを実行し、表示部１４に指紋情報の取得要求を表示する（ステップＳ１６４）。表示する内容は予めＲＯＭ５５に記憶されており、「例えば、指紋取得部に親指をおいて下さい。」等の情報を読み出して表示部１４へ出力するようにすればよい。指紋取得部１１２から指紋情報が入力された場合、セキュリティチップ５のＭＰＵ５１は指紋情報を

受け付け、ＲＡＭ５２に一時的に記憶する（ステップＳ１６５）。

【００７５】

そして、セキュリティチップ５のＭＰＵ５１は携帯電話機１の環境情報を取得する（ステップＳ１６６）。環境情報の収集は、上述したようにＭＰＵ５１が携帯電話機１のＲＯＭ１５のＯＳ、ＢＩＯＳ及びインストールされるソフトウェアを常駐して監視し、携帯電話機１の機器名、ＯＳの名称、バージョン、外部接続端子１９に接続された周辺機器の機器名、バージョン、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル５５１に記憶される（ステップＳ１６７）。

【００７６】

セキュリティチップ５のＭＰＵ５１はＲＡＭ５２に記憶した生体情報及び環境情報ファイル５５１に記憶した環境情報を読み出す（ステップＳ１６８）。セキュリティチップ５のＭＰＵ５１は、読み出した生体情報及び環境情報に、ＲＯＭ５５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ１６９）。ＭＰＵ５１は認証機関サーバ３から予め発行を受けた携帯電話機１の個人鍵を個人鍵ファイル５５４から読み出し、生体情報及び環境情報並びにメッセージダイジェストを暗号化する（ステップＳ１７１）。さらに、ＭＰＵ５１は電子証明書ファイル５５３から認証機関サーバ３において予め発行を受けた電子証明書を読み出し、暗号化した生体情報及び環境情報並びにメッセージダイジェストに電子証明書を添付して中央サーバ２へ送信する（ステップＳ１７２）。中央サーバ２のＣＰＵ２１は送信された電子証明書、暗号化された生体情報及び環境情報並びにメッセージダイジェストをＲＡＭ２２に記憶する。なお、本実施の形態においては生体情報及び環境情報の双方を暗号化して送信しているが、生体情報または環境情報のいずれか一方のみを暗号化して送信するようにしても良い。

【００７７】

中央サーバ２のＣＰＵ２１は電子証明書に記載されている認証機関サーバ３へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求す

る（ステップＳ１７３）。認証機関サーバ３は、電子証明書の公開鍵を中央サーバ２へ送信し、中央サーバ２は送信された電子証明書の公開鍵を受信する（ステップＳ１７４）。中央サーバ２のＣＰＵ２１は、記憶した電子証明書をＲＡＭ２２から読み出し、認証機関サーバ３から送信された認証機関の公開鍵を用いて電子証明書を復号し携帯電話機１の公開鍵を取得する（ステップＳ１７５）。

【００７８】

中央サーバ２のＣＰＵ２１は取得した携帯電話機１の公開鍵を用いて暗号化された生体情報及び環境情報並びにメッセージダイジェストを復号する（ステップＳ１８１）。さらにＣＰＵ２１は復号した生体情報及び環境情報に、中央サーバ２の記憶部２５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ１８２）。中央サーバ２のＣＰＵ２１はステップＳ１８１で復号したメッセージダイジェストと、ステップＳ１８２で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある顧客の携帯電話機１から情報が送受信されたものであるか否かを判断する（ステップＳ１８３）。

【００７９】

メッセージダイジェストが一致しない場合は（ステップＳ１８３でＮＯ）、ＣＰＵ２１は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップＳ１８５）。一方、メッセージダイジェストが一致する場合は（ステップＳ１８３でＹＥＳ）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップＳ１８４）。そして、中央サーバ２のＣＰＵ２１は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）を記憶部２５に記憶する（ステップＳ１８６）。

【００８０】

続いて、中央サーバ２のＣＰＵ２１は指紋情報ファイル２５２から予め登録された認証用の指紋情報を読み出す（ステップＳ１８７）。ＣＰＵ２１は復号した指紋情報と、読み出した認証用の指紋情報とを比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップＳ１９１）。

【００８１】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップＳ１９１でＹＥＳ）、指紋認証適正フラグをセットする（ステップＳ１９２）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップＳ１９１でＮＯ）、指紋認証不適正フラグをセットする（ステップＳ１９３）。中央サーバ２のＣＰＵ２１は指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部２５に記憶する（ステップＳ１９４）。

【００８２】

中央サーバ２のＣＰＵ２１はステップＳ１６２で決定した階級に対応する環境情報の条件を環境情報ＤＢ２５１から読み出す（ステップＳ１９５）。そして、ＣＰＵ２１は、復号された環境情報が、ステップＳ１９５にて読み出された環境情報の条件を満たすか否かを判断する（ステップＳ１９６）。条件を満たさない場合（ステップＳ１９６でＮＯ）、環境認証不適正フラグをセットする（ステップＳ１９８）。一方、条件を満たす場合（ステップＳ１９６でＹＥＳ）、環境認証適正フラグをセットする（ステップＳ１９７）。中央サーバ２のＣＰＵ２１は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部２５に記憶する（ステップＳ２０１）。

【００８３】

ＣＰＵ２１は、記憶部２５に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップＳ２０２）。全ての適正フラグがセットされている場合（ステップＳ２０２でＹＥＳ）、携帯電話機１を安全なものと判断し安全フラグをセットする（ステップＳ２０３）。換言すれば、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の全てにおいて適正と判断された場合に限り携帯電話機１を適正なものであると判断する。中央サーバ２のＣＰＵ２１は携帯電話機１またはＷｅｂサーバ４に通信を継続することを示す信号を送信する（ステップＳ２０４）。

【００８４】

一方、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の内、１つ

でも不適正フラグがセットされている場合は、不適正フラグをセットする（ステップＳ２０５）。この場合ＣＰＵ２１は携帯電話機１またはＷｅｂサーバ４に通信を終了することを示す信号を送信する（ステップＳ２０６）。

【００８５】

実施の形態４

実施の形態４は、パッチ用のソフトウェア、ファームウェアを提供する場合に適用される安全性判断システムに関する。ＰＤＡ、携帯電話機、冷蔵庫、空気調和機、プリンタ等においては、内蔵されるソフトウェアのバグが発見される場合があり、この場合、パッチ用のソフトウェアを提供する必要がある。また、追加機能を備えるファームウェアを提供する場合もある。実施の形態４では安全性を確保した上でこれらのソフトウェアを顧客に提供することが可能な安全性判断システムについて説明する。

【００８６】

図２１は実施の形態４に係る携帯電話機１のハードウェア構成を示すブロック図である。図２１に示す１１４は携帯電話機エンジン部１１０に電力を供給する主電力供給手段（以下、主電源部という）であり、リチウム電池等が用いられる。入力部１３の図示しないオンボタンの操作により、主電源部１１４から携帯電話機エンジン部１１０及びセキュリティチップ５へ電力が供給され、図示しないオフボタンの操作により、主電源部１１４から携帯電話機エンジン部１１０及びセキュリティチップ５への電力が遮断され携帯電話機１の電源が切られる。

【００８７】

一方、副電力供給手段（以下、副電源部という）１１５は、例えばコイン形のリチウム電池が用いられ、主電源部１１４による携帯電話機エンジン部１１０及びセキュリティチップ５への電力供給が行われていない場合にでも、蓄積手段としての第２ＲＯＭ１１６及び受信通信手段としての副アンテナ部１１７に電力を供給する。主電源部１１４により電力が供給されている場合、すなわち携帯電話機の電源がオンの場合に、中央サーバ２からソフトウェアが送信されたときは、該ソフトウェアはアンテナ部１６からソフトウェアを受信し、ＣＰＵ１１がＲＯＭ１５にソフトウェアを記憶する。この場合、副電源部１１５による電力供給は

行われていない。

【００８８】

逆に、主電源部１１４による電力供給がなされていない場合、すなわち携帯電話機１の電源がオフの場合、副電源部１１５により、副アンテナ部１１７及び第２ＲＯＭ１１６に電源が供給される。そして、中央サーバ２からソフトウェアが送信された場合、副アンテナ部１１７でソフトウェアを受信し、第２ＲＯＭ１１６に受信したソフトウェアを記憶し、主電源による電力が供給された時点で、第２ＲＯＭ１１６に記憶したソフトウェアをＲＯＭ１５に書き込む処理を行う。なお、副アンテナ部１１７は、例えば公知のＦＭ文字多重放送受信モジュールを用いればよい。この場合、中央サーバはＦＭ放送局を介してソフトウェアを含むＦＭ文字放送を発信する。副アンテナ部１１７であるＦＭ文字多重放送受信モジュールが、ＦＭ文字放送を受信した場合、ＤＡＲＣ規格の文字コードで記述されたソフトウェアのデータを、Ｃ言語、Ｊａｖａ等で記述されたソースコードに変換する。最後にセキュリティチップ５のＭＰＵ５１は本人認証、ＰＫＩ認証及び環境認証を行った上で、ＲＯＭ１５にソフトウェアをインストールする。

【００８９】

図２２は中央サーバ２のハードウェア構成を示すブロック図である。図２２に示すように記憶部２５には、認証機関サーバ３による認証を経たパッチ用のソフトウェア、ファームウェア、プラグインソフト、ワクチン等の数々のソフトウェアが記憶されている。なお、これらのソフトウェアはソフトウェア会社から提供をうけている。電子証明書ファイル２５３には、予め認証機関サーバ３から発行を受けた中央サーバ２の電子証明書が記憶されており、個人鍵ファイル２５４にも同じく、予め認証機関サーバ３から発行を受けた中央サーバ２の個人鍵が記憶されている。

【００９０】

以上のハードウェア構成において安全性が保証されたソフトウェアの提供処理について、フローチャートを用いて説明する。図２３乃至図２９は実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。まず、中央サーバ２のＣＰＵ２１は携帯電話機１に発呼するなどして、主電源がオンかオフか

の情報の取得要求を行う（ステップＳ２３１）。携帯電話機１は主電源がオンかオフの情報を送信する（ステップＳ２３２）。中央サーバ２は主電源がオンであるか否かを判断し（ステップＳ２３３）、主電源がオンである場合（ステップＳ２３３でＹＥＳ）、ステップＳ１６２で説明した如く安全性の階級を決定する（ステップＳ２３４）。この安全性に関しては提供されるソフトウェアの重要度に応じて管理者が決定するようにすればよい。例えばパッチ用ソフトウェアまたはワクチンソフトの場合は安全性を高めるべく階級１と決定され、ゲーム用のソフトウェアなど安全性が低いものは階級６と決定される。

【００９１】

中央サーバ２のＣＰＵ２１は認証開始信号を携帯電話機１へ送信する（ステップＳ２３５）。認証開始信号を受信したセキュリティチップ５のＭＰＵ５１は、制御プログラム５５Ｐを実行し、表示部１４に指紋情報の取得要求を表示する（ステップＳ２３６）。指紋取得部１１２から指紋情報が入力された場合、セキュリティチップ５のＭＰＵ５１は指紋情報を受け付け（ステップＳ２３７）、ＲＡＭ５２に一時的に記憶する。そして、ＭＰＵ５１はＲＯＭ５５の指紋情報ファイル５５２に携帯電話機１の購入時に予め記憶してある指紋情報を読み出し、ＲＡＭ５２に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップＳ２４１）。

【００９２】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップＳ２４１でＹＥＳ）、指紋認証適正フラグをセットする（ステップＳ２４３）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップＳ２４１でＮＯ）、指紋認証不適正フラグセットする（ステップＳ２４２）。ＭＰＵ５１は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部５５に記憶する（ステップＳ２４４）。

【００９３】

次に、セキュリティチップ５のＭＰＵ５１は携帯電話機１の環境情報を取得する（ステップＳ２４５）。収集された環境情報は環境情報ファイル５５１に記憶される（ステップＳ２４６）。ＭＰＵ５１は環境情報ファイル５５１から収集し

た環境情報を読み出して中央サーバ２へ送信する（ステップＳ２４７）。中央サーバ２のＣＰＵ２１は送信された環境情報をＲＡＭ２２に記憶する。中央サーバ２のＣＰＵ２１はステップＳ１６２にて決定した階級に対応する環境情報の条件を環境情報ＤＢ２５１から読み出す（ステップＳ２４８）。

【００９４】

そして、ＣＰＵ２１は、ＲＡＭ２２に記憶され、受信した環境情報が、読み出した環境情報の条件を満たすか否かを判断する（ステップＳ２５１）。条件を満たさない場合（ステップＳ２５１でＮＯ）、環境認証不適正フラグをセットする（ステップＳ２５３）。一方、条件を満たす場合（ステップＳ２５１でＹＥＳ）、環境認証適正フラグをセットする（ステップＳ２５２）。中央サーバ２のＣＰＵ２１は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部２５に記憶し（ステップＳ２５４）、携帯電話機１へ送信する（ステップＳ２５５）。環境認証のフラグを受信したセキュリティチップ５のＭＰＵ５１は、環境認証フラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部５５に記憶する（ステップＳ２５６）。

【００９５】

さらに中央サーバ２のＣＰＵ２１は記憶部２５に記憶した提供用のソフトウェアを記憶部２５から読み出す（ステップＳ２５７）。ＣＰＵ２１は、読み出したソフトウェアに、記憶部２５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ２５８）。ＣＰＵ２１は認証機関サーバ３から予め発行を受けた中央サーバ２の個人鍵を個人鍵ファイル２５４から読み出し、ソフトウェア及びメッセージダイジェストを暗号化する（ステップＳ２５９）。ＣＰＵ２１は電子証明書ファイル２５３から認証機関サーバ３において予め発行を受けた電子証明書を読み出し、暗号化したソフトウェア及びメッセージダイジェストに電子証明書を添付して携帯電話機１へ送信する（ステップＳ２６１）。セキュリティチップ５のＭＰＵ５１は送信された電子証明書、暗号化されたソフトウェア及びメッセージダイジェストをＲＡＭ５２に記憶する。

【００９６】

セキュリティチップ５のＭＰＵ５１は電子証明書に記載されている認証機関サ

ーバ３へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求する（ステップＳ２６２）。認証機関サーバ３は、電子証明書の公開鍵を携帯電話機１へ送信し、セキュリティチップ５のＭＰＵ５１は送信された公開鍵を受信する（ステップＳ２６３）。ＭＰＵ５１は記憶した電子証明書をＲＡＭ５２から読み出し、認証機関サーバ３から送信された認証機関の公開鍵を用いて電子証明書を復号し中央サーバ２の公開鍵を取得する（ステップＳ２６４）。

【００９７】

セキュリティチップ５のＭＰＵ５１は取得した中央サーバ２の公開鍵を用いて、暗号化されたソフトウェア及びメッセージダイジェストを復号する（ステップＳ２６５）。さらにＭＰＵ５１は復号したソフトウェアに、セキュリティチップ５のＲＯＭ５５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ２６６）。ＭＰＵ５１はステップＳ２６５で復号したメッセージダイジェストと、ステップＳ２６６で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある中央サーバ２から情報が送受信されたものであるか否かを判断する（ステップＳ２７１）。

【００９８】

メッセージダイジェストが一致しない場合は（ステップＳ２７１でＮＯ）、ＭＰＵ５１は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップＳ２７２）。一方、メッセージダイジェストが一致する場合は（ステップＳ２７１でＹＥＳ）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップＳ２７３）。そして、セキュリティチップ５のＭＰＵ５１は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）をＲＯＭ５５に記憶する（ステップＳ２７４）。

【００９９】

ＭＰＵ５１はＲＯＭ５５に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステ

ップＳ２７５）。全ての適正フラグがセットされている場合（ステップＳ２７５でＹＥＳ）、送信されたソフトウェアを安全なものと判断し安全フラグをセットする（ステップＳ２７８）。セキュリティチップ５のＭＰＵ５１はステップＳ２６５で復号されたソフトウェアを携帯電話機エンジン部１１０のＲＯＭ１５にインストールする（ステップＳ２７１０）。そして、ＭＰＵ５１はインストールが完了したことを示す信号を中央サーバ２へ送信する（ステップＳ２７１１）。

【０１００】

一方、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の内、１つでも不適正フラグがセットされている場合（ステップＳ２７５でＮＯ）は、不適正フラグをセットする（ステップＳ２７９）。この場合ＭＰＵ５１はインストールを拒否することを示す信号を中央サーバ２へ送信する（ステップＳ２７１２）。

【０１０１】

ステップＳ２３３でＮＯの場合、つまり携帯電話機１の主電源がオフの場合、中央サーバ２のＣＰＵ２１は記憶部２５に記憶した提供用のソフトウェアを記憶部２５から読み出す（ステップＳ２８１）。ＣＰＵ２１は、読み出したソフトウェアに、記憶部２５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ２８２）。ＣＰＵ２１は認証機関サーバ３から予め発行を受けた中央サーバ２の個人鍵を個人鍵ファイル２５４から読み出し、ソフトウェア及びメッセージダイジェストを暗号化する（ステップＳ２８３）。ＣＰＵ２１は電子証明書ファイル２５３から認証機関サーバ３において予め発行を受けた電子証明書を読み出し、暗号化したソフトウェア及びメッセージダイジェストに電子証明書を添付して、ＦＭ放送局のコンピュータ（図示せず）へ送信する（ステップＳ２８４）。

【０１０２】

ＦＭ放送局のコンピュータは電子証明書、暗号化されたソフトウェア及びメッセージダイジェストをＤＡＲＣ規格の放送データに変換し、ＦＭ文字放送多重回路（図示せず）によってＦＭ音楽データと放送データとに多重化する。これらのデータはＦＭ変調発振器によりＦＭ変調されて放送される。携帯電話機１は副ア

ンテナ部１１７からＦＭ文字放送を受信し（ステップＳ２８５）、ＤＡＲＣ規格の文字コードで記述されたデータを変換して電子証明書、暗号化したソフトウェア及びメッセージダイジェストを取り出す。なお、ＤＡＲＣ規格を利用したＦＭ文字放送に関する技術は特開平１０－１１６２３７号に開示されている。

【０１０３】

変換された、電子証明書、ソフトウェア及びメッセージダイジェストは第２ＲＯＭ１１６に記憶される（ステップＳ２８６）。そして顧客の入力部１３の操作により、主電源部１１４による電力の供給が開始された場合（ステップＳ２９１）、ステップＳ２３６～ステップＳ２４４で説明した処理と同様に指紋認証を行い（ステップＳ２９２）、ステップＳ２４５～ステップＳ２５６で説明した処理と同様に環境認証を行い（ステップＳ２９４）、ステップＳ２６２～ステップＳ２７４で説明した処理と同様に電子証明書による認証を行う（ステップＳ２９３）。なお、電子証明書による認証を行う場合は、ＣＰＵ５１が第２ＲＯＭ１１６に記憶された電子証明書、暗号化されたソフトウェア及びメッセージダイジェストを読み出して、ＲＡＭ５２に記憶してから、電子証明書による認証を行う。つまり、認証機関サーバ３から取得した公開鍵を用いて、電子証明書から公開鍵を取得し、取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。

【０１０４】

ＭＰＵ５１はＲＯＭ５５に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップＳ２９５）。全ての適正フラグがセットされている場合（ステップＳ２９５でＹＥＳ）、送信されたソフトウェアを安全なものと判断し安全フラグをセットする（ステップＳ２９６）。セキュリティチップ５のＭＰＵ５１は復号されたソフトウェアを携帯電話機エンジン部１１０のＲＯＭ１５にインストールする（ステップＳ２９８）。そして、ＭＰＵ５１はインストールが完了したことを示す信号を中央サーバ２へ送信する（ステップＳ２９９）。

【０１０５】

一方、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の内、１つでも不適正フラグがセットされている場合（ステップＳ２９５でＮＯ）は、不適正フラグをセットする（ステップＳ２９７）。この場合ＭＰＵ５１はインストールを拒否することを示す信号を中央サーバ２へ送信する（ステップＳ２９１０）。

【０１０６】

中央サーバ２から提供されるソフトウェアはパッチ用ソフトウェア等の他、ＤＤｏＳ攻撃の対象となった携帯電話機１内のソフトウェアを削除するためのソフトウェアであっても良い。例えば、何らかの原因により、携帯電話機１に数日後に所定のＷｅｂサーバにＤＤｏＳ攻撃を行うソフトウェア（プログラム）がセットされた場合、本発明の認証を経たソフトウェアを提供する。提供されるソフトウェアには、日時情報が記憶されており、インストールして実行することにより記憶された日時以降に記憶されたデータを全て消去する。

【０１０７】

図３０はインストールされた消去用ソフトウェアの処理内容を示すフローチャートである。ステップＳ２９８によりＲＯＭ１５に消去用のソフトウェアがインストールされる。顧客は消去用のソフトウェアを、入力部１３を操作することによりＣＰＵ１１に実行させる（ステップＳ３０１）。ＣＰＵ１１はＲＯＭ１５内の記憶履歴の読み出しを行う（ステップＳ３０２）。具体的には記憶されたファイル、インストールされたソフトウェア等のデータと、さらにそれらのデータが記憶された日時の情報を読み出す。ＣＰＵ１１は消去用のソフトウェアの実行プログラムから日時の情報を読み出す（ステップＳ３０３）。そして読み出した記憶履歴を参照し、読み出した日時以降に記憶されたデータを全て消去する（ステップＳ３０４）。これにより、ＤＤｏＳ攻撃の踏み台にされた携帯電話機１が、攻撃に利用されることを防止することができる。

【０１０８】

実施の形態５

図３１は実施の形態５に係る携帯電話機１のハードウェア構成を示すブロック図である。実施の形態４に係る携帯電話機１を実行させるためのコンピュータプ

ログラムは、本実施の形態５のように携帯電話機１にプレインストールして提供することも、またＣＤ－ＲＯＭ、ＭＯ、メモリーカード等の可搬型記録媒体で提供することも可能である。さらに、コンピュータプログラムを回線経由で搬送波として伝搬させて提供することも可能である。すなわち、セキュリティチップ５を搭載する代わりに、セキュリティチップ５と同様の機能をもつコンピュータプログラムを携帯電話機１のＲＯＭ１７にインストールするようにしても良い。以下に、その内容を説明する。

【０１０９】

図３１に示す携帯電話機１に、生体情報を認証させ、環境情報を収集させ、環境情報を送信させ、電子証明書による認証をさせ、インストールさせるプログラムが記録された記録媒体１ａ（ＣＤ－ＲＯＭ、ＭＯ、メモリーカード又はＤＶＤ－ＲＯＭ等）が携帯電話機１のＲＯＭ１５にインストールされている。インストールの方法としては、外部接続端子１９に接続可能なメモリーカード等の記録媒体１ａを嵌挿し、プログラムをインストールするか、または、中央サーバ２から本発明に係るプログラムをダウンロードするようにしても良い。係るプログラムは携帯電話機１のＲＡＭ１２にロードして実行される。これにより、上述のような本発明の情報処理装置としての携帯電話機１として機能する。

【０１１０】

実施の形態６

本実施の形態においては、携帯電話機１及び中央サーバ２の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機１及び中央サーバ２を安全と判断しその後の情報の送受信を許可する技術について説明する。

【０１１１】

図３２は実施の形態６に係る携帯電話機１のハードウェア構成を示すブロック図であり、また図３３は実施の形態６に係る中央サーバ２のハードウェア構成を示すブロック図である。図３２に示すように本実施の形態においては携帯電話機１においても中央サーバ２の環境認証を行うため、携帯電話機１のＲＯＭ１５には環境情報ＤＢ１５１が用意されている。図４で説明したものと同様に、中央サ

ーバ２の外部通信ポート２９に接続される周辺機器、ＰＣカード（図示せず）、インストールされているＯＳ，ソフトウェア等に対する環境情報に対する条件が、セキュリティポリシィである階級に対応付けられて記憶されている。

【０１１２】

中央サーバ２も携帯電話機１による認証を受けるべく、指紋取得部２１２及びセキュリティチップ５がバス２７を介してＣＰＵ２１に接続されている。なお、これらの詳細については既に実施の形態１で説明したとおりであるので詳細な説明は省略する。また２９はＵＳＢポート、ＲＳ２３２Ｃポート等の外部通信ポートであり、プリンタ、マウス、ハードディスク、ＭＯ等の周辺機器が接続される。

【０１１３】

本実施の形態においては、携帯電話機１及び中央サーバ２の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機１及び中央サーバ２を安全と判断しその後の情報の送受信を許可するために、図１１に示すステップＳ１１５以降に、すなわち携帯電話機１の安全性が確認された後に、以下の処理を追加して行う。

【０１１４】

図３４乃至図３７は実施の形態６に係る認証処理の手順を示すフローチャートである。ステップＳ１１５の後、中央サーバ２のセキュリティチップ５のＭＰＵ５１は制御プログラム５５Ｐを実行し、表示部２４に指紋情報の取得要求を表示する（ステップＳ３４１）。指紋取得部２１２から指紋情報が入力された場合、セキュリティチップ５のＭＰＵ５１は指紋情報を受け付け（ステップＳ３４２）、ＲＡＭ５２に一時的に記憶する。そして、ＭＰＵ５１はＲＯＭ５５の指紋情報ファイル５５２に携帯電話機１の購入時に予め記憶してある指紋情報を読み出し、ＲＡＭ５２に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップＳ３４３）。

【０１１５】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップＳ３４３でＹＥＳ）、指紋認証適正フラグをセットし、セットした指紋認証適正フラグ

を携帯電話機１へ送信する（ステップＳ３４５）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップＳ３４３でＮＯ）、指紋認証不適正フラグセットし、セットした指紋認証不適正フラグを携帯電話機１へ送信する（ステップＳ３４４）。携帯電話機１のＣＰＵ１１は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）をＲＯＭ１５に記憶する（ステップＳ３４６）。なお、本実施の形態においては指紋を用いた生体認証を中央サーバ２において実行することとしたが、予め採取した指紋情報を認証機関サーバ３または携帯電話機１に記憶しておき、認証機関サーバ３または携帯電話機１において判断するようにしても良い。これにより指紋を用いた生体認証が終了する。

【０１１６】

続いて、セキュリティチップ５のＭＰＵ５１は中央サーバ２の環境情報を取得する（ステップＳ３４７）。環境情報の収集は、上述したようにＭＰＵ５１が中央サーバ２のＲＯＭ１５のＯＳ、ＢＩＯＳ及びインストールされるソフトウェアを常駐して監視し、中央サーバ２の機器名、ＯＳの名称、バージョン、外部通信ポート２９に接続された周辺機器の機器名、バージョン、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル５５１に記憶される（ステップＳ３４８）。

【０１１７】

セキュリティチップ５のＭＰＵ５１はＲＡＭ５２に記憶した環境情報ファイル５５１に記憶した環境情報を読み出す（ステップＳ３４９）。セキュリティチップ５のＭＰＵ５１は、読み出した環境情報に、ＲＯＭ５５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ３５１）。ＭＰＵ５１は認証機関サーバ３から予め発行を受けた中央サーバ２の個人鍵を個人鍵ファイル５５４から読み出し、環境情報及びメッセージダイジェストを暗号化する（ステップＳ３５２）。さらに、ＭＰＵ５１は電子証明書ファイル５５３から認証機関サーバ３において予め発行を受けた電子証明書を読み出し、暗号化した環境情報及びメッセージダイジェストに電子証明書を添付して携帯電話機１へ送信す

る（ステップＳ３５３）。携帯電話機１のＣＰＵ１１は送信された電子証明書、暗号化された環境情報及びメッセージダイジェストをＲＡＭ１２に記憶する。

【０１１８】

携帯電話機１のＣＰＵ１１は電子証明書に記載されている認証機関サーバ３へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求する（ステップＳ３５４）。認証機関サーバ３は、電子証明書の公開鍵を携帯電話機１へ送信し、携帯電話機１は送信された電子証明書の公開鍵を受信する（ステップＳ３５５）。携帯電話機１のＣＰＵ１１は、記憶した電子証明書をＲＡＭ１２から読み出し、認証機関サーバ３から送信された認証機関の公開鍵を用いて電子証明書を復号し中央サーバ２の公開鍵を取得する（ステップＳ３５６）。

【０１１９】

携帯電話機１のＣＰＵ１１は取得した中央サーバ２の公開鍵を用いて暗号化された環境情報及びメッセージダイジェストを復号する（ステップＳ３６１）。さらにＣＰＵ１１は復号した環境情報に、携帯電話機１のＲＯＭ５５に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップＳ３６２）。携帯電話機１のＣＰＵ１１はステップＳ３６１で復号したメッセージダイジェストと、ステップＳ３６２で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある中央サーバ２から情報が送受信されたものであるか否かを判断する（ステップＳ３６３）。

【０１２０】

メッセージダイジェストが一致しない場合は（ステップＳ３６３でＮＯ）、ＣＰＵ１１は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップＳ３６５）。一方、メッセージダイジェストが一致する場合は（ステップＳ３６３でＹＥＳ）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップＳ３６４）。そして、携帯電話機１のＣＰＵ１１は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）をＲＯＭ１５に記憶する（ステップＳ３６６）。

【０１２１】

携帯電話機１のＣＰＵ１１はステップＳ１０４で決定した階級に対応する環境情報の条件を環境情報ＤＢ１５１から読み出す（ステップＳ３７１）。そして、ＣＰＵ１１は、復号された環境情報が、ステップＳ３７１にて読み出された環境情報の条件を満たすか否かを判断する（ステップＳ３７２）。条件を満たさない場合（ステップＳ３７２でＮＯ）、環境認証不適正フラグをセットする（ステップＳ３７４）。一方、条件を満たす場合（ステップＳ３７２でＹＥＳ）、環境認証適正フラグをセットする（ステップＳ３７３）。携帯電話機１のＣＰＵ１１は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）をＲＯＭ１５に記憶する（ステップＳ３７５）。

【０１２２】

ＣＰＵ１１は、ＲＯＭ１５に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップＳ３７６）。全ての適正フラグがセットされている場合（ステップＳ３７６でＹＥＳ）、中央サーバ２を安全なものと判断し安全フラグをセットし、ステップＳ１２１へ移行する（ステップＳ３７７）。

【０１２３】

一方、生体認証、電子証明書認証（ＰＫＩ認証）、および環境認証の内、１つでも不適正フラグがセットされている場合（ステップＳ３７６でＮＯ）は、不適正フラグをセットし、ステップＳ１２３へ移行する（ステップＳ３７８）。このように、携帯電話機１及び中央サーバ２の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に限り、携帯電話機１及び中央サーバ２を安全と判断しその後の情報の送受信を許可するようにしたので、より安全性の高い通信環境を提供することが可能となる。

【０１２４】

なお、本実施の形態においては、携帯電話機１及び中央サーバ２の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機１及び中央サーバ２を安全と判断しその後の情報の送受信を許可する技術について説明したが、同様に携帯電話機１及びオンラインショップのＷｅｂサー

バ４間（または図示しない他の携帯電話機、洗濯機、パーソナルコンピュータ等の情報処理装置）についても、双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機１及びＷｅｂサーバ４等を安全と判断しその後の情報の送受信を許可するようにしても良いことは言うまでもない。

【０１２５】

実施の形態２乃至６は以上の如き構成としてあり、その他の構成及び作用は実施の形態１と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

（付記１）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、

予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、

前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステッ

プによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

（付記２）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第１認証装置へ送信する環境情報送信ステップと、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第１認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第１認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記情報処理装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップと

を備えることを特徴とする安全性判断方法。

（付記３）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法におい

て、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第１認証装置または第２認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を、前記第２認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、

予め前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第１認証装置へ送信する暗号化情報送信ステップと、

前記第１認証装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第１認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第１認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

（付記４）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

（付記５）　前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第１認証装置へ送信するよう構成してあることを特徴とする付記４に記載の安全性判断システム。

（付記６）　前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、

前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付ける手段をさらに備え、

前記暗号化情報送信手段は、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第１認証装置へ送信するよう構成してあり、

前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、

前記第１認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送

信する手段をさらに備えることを特徴とする付記４に記載の安全性判断システム。

（付記７）　前記第１認証装置は、

生体情報を受け付ける副生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、

前記第２認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第１認証装置を安全と判断する副安全判断手段と

を備えることを特徴とする付記４に記載の安全性判断システム。

（付記８）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境

情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記情報処理装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備える

ことを特徴とする安全性判断システム。

（付記９）　前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給をうける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする付記８に記載の安全性判断システム。

（付記１０）　前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第２認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断するよう構成してあることを特徴とする付記９に記載の安全判断システム。

（付記１１）　前記ソフトウェアは、前記情報処理装置に予めインストール

されているソフトウェアのパッチ用ソフトウェアであることを特徴とする付記８乃至１０に記載の安全判断システム。

（付記１２）　前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶されたデータを消去する消去手段をさらに備えることを特徴とする付記８乃至１０に記載の安全判断システム。

（付記１３）　情報処理装置、第１認証装置及び第２認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

前記第２認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第１認証装置へ送信する暗号化情報送信手段とを備え、

前記第１認証装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

（付記１４）　前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする付記４乃至１３のいずれかに記載の安全判断システム。

（付記１５）　前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする付記４乃至１４のいずれかに記載の安全判断システム。

（付記１６）　第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信する暗号化情報送信手段と、

前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第１認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断装置。

（付記１７）　第１認証装置及び第２認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第１認証装置へ送信する環境情報送信手段と、

前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて電子証明書から取得した公開

鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断され、また前記環境情報送信手段により送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段と

を備えることを特徴とする安全性判断装置。

（付記１８）　通信網を介して接続される情報処理装置の安全性を判断する第１認証装置において、

前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、

通信網を介して接続された第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理から送信された場合に、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、

前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする第１認証装置。

（付記１９）　第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第１認証装置へ送信させる暗号化情報送信ステップと、

コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第１認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第１認証装置により適正と判断され、前記第１認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップと

を実行させることを特徴とするコンピュータプログラム。

（付記２０）　第１認証装置及び第２認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第１認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第１認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第２認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、

コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第１認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストー

ルするインストールステップと

を実行させることを特徴とするコンピュータプログラム。

（付記２１）　前記第１認証装置により、生体情報を受け付ける副生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、第１認証装置または第２認証装置により判断する副生体情報認証ステップと、

前記第１認証装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集ステップと、

前記第２認証装置から発行を受けた個人鍵で前記副環境情報収集ステップにより収集した環境情報を暗号化する副暗号化ステップと、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信ステップと、

前記情報処理装置により、前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記情報処理装置により前記送信された環境情報が適正であるか否かを判断する副環境情報認証ステップと、

前記副生体情報認証ステップ、副環境情報認証ステップ及び副電子証明書認証ステップによる認証が全て適正であり、かつ前記安全判断ステップにより安全と判断された場合に、前記情報処理装置及び前記第１認証装置を安全と判断する副安全判断ステップと

を備えることを特徴とする付記１または３に記載の安全性判断方法。

（付記２２）　前記第１認証装置は、

生体情報を受け付ける副生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、

前記第２認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、

前記第２認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第２認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第１認証装置を安全と判断する副安全判断手段と

を備えることを特徴とする付記１２に記載の安全判断システム。

【０１２６】

【発明の効果】

以上詳述した如く、本発明にあっては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かを判断する。また、情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する。情報処理装置は収集した環境情報を第１認証装置へ送信する。さらに、第２認証装置から発行を受けた電子証明書及び情報処理装置の個人鍵で暗号化された商取引に関する情報等を第１認証装置へ送信する。第１認証装置は、電子証明書及び暗号化された情報を受信した場合、第２認証装置から取得した第２認証装置（認証機関）の公開鍵を用いて、送信された電子証明書から情報処理装置の公開鍵を取得する。そして、取得した情報処理装置の公開鍵で暗号化された情報を復号し、復号された情報が適正であるか否かを判断する。

【０１２７】

第１認証装置は、送受信される情報に応じて階級付けされた環境情報の条件を

記憶した環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。そして、生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置を安全と判断する。このように構成したので、情報処理装置の安全性を確保しつつ、円滑な情報の送受信及び商取引を実現することが可能となる。さらに、第１認証装置においても生体情報認証、電子証明書認証及び環境認証をおこない、情報処理装置における生体情報認証、電子証明書認証及び環境認証、並びに、第１に認証装置における生体情報認証、電子証明書認証及び環境認証において、全て適正と判断された場合のみ、第１認証装置及び情報処理装置の双方を安全と判断するようにしたので、さらに高度な安全性を確保することが可能となる。

【０１２８】

また、本発明にあっては、利用者の生体情報を受け付け、受け付けた生体情報が適正であるか否かの本人認証を行う。そして情報処理装置は収集した環境情報を第１認証装置へ送信し、第１認証装置において、環境情報の認証を行う。第１認証装置から情報処理装置へパッチ用のソフトウェア等を送信する場合は、第１認証装置は、第２認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを情報処理装置へ送信する。情報処理装置は、電子証明書及び暗号化されたソフトウェアを受信した場合、第２認証装置へ公開鍵を要求し、この認証機関の公開鍵を用いて電子証明書から第１認証装置の公開鍵を取得する。そしてこの公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。最後に、上述した本人認証、環境認証及び電子証明書による認証が全て適正であると判断した場合、復号したソフトウェアを情報処理装置へインストールする。このように構成したので、第３者のなりすましを防止でき、高度な安全性を維持した上で情報処理装置へパッチ用のソフトウェア、ファームウェア等のソフトウェアを提供することが可能となる。

【０１２９】

さらに、本発明にあっては、情報処理装置は、主電力供給手段及び副電力供給手段を備え、受信用通信手段は副電力供給手段から電力の供給をうける構成としている。主電力供給手段による電力の供給が行われていない場合、すなわちメイ

ンの電源がオンにされていない場合に、第１認証装置から電子証明書及び個人鍵で暗号化されたソフトウェアが送信された場合は、サブバッテリーを用いた受信用通信手段によりこれらの情報を受信して蓄積する。そして、主電力供給手段による電力の供給が行われた場合に、蓄積した電子証明書及びソフトウェアを読み出し、送信されたソフトウェアが適正であるか否かの判断、本人認証及び環境認証を行うようにしたので、電源をオンにしていない顧客に対してもパッチ用のソフトウェアを、安全性を確保した上で大量に配布することが可能となる。また特に提供するソフトウェアとして、所定の日時以降に記憶されたデータを記憶部から消去するソフトウェアを提供することによりＤＤｏＳ攻撃の踏み台にされることを効果的に防止することが可能となる等、本発明は優れた効果を奏し得る。

【図面の簡単な説明】

【図１】

本発明に係る安全性判断システムの概要を示す模式図である。

【図２】

携帯電話機のハードウェア構成を示すブロック図である。

【図３】

中央サーバのハードウェア構成を示すブロック図である。

【図４】

環境情報ＤＢのレコードレイアウトを示す説明図である。

【図５】

Ｗｅｂサーバと携帯電話機との間の商取引の手順を示すフローチャートである。

【図６】

Ｗｅｂページのイメージを示す説明図である。

【図７】

安全性の判断処理の手順を示すフローチャートである。

【図８】

安全性の判断処理の手順を示すフローチャートである。

【図９】

安全性の判断処理の手順を示すフローチャートである。

【図１０】

安全性の判断処理の手順を示すフローチャートである。

【図１１】

安全性の判断処理の手順を示すフローチャートである。

【図１２】

安全性の判断処理の手順を示すフローチャートである。

【図１３】

実施の形態２に係る携帯電話機のハードウェア構成を示すブロック図である。

【図１４】

実施の形態３に係る携帯電話機のハードウェア構成を示すブロック図である。

【図１５】

中央サーバのハードウェア構成を示すブロック図である。

【図１６】

実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。

【図１７】

実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。

【図１８】

実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。

【図１９】

実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。

【図２０】

実施の形態３に係る安全性の判断処理の手順を示すフローチャートである。

【図２１】

実施の形態４に係る携帯電話機のハードウェア構成を示すブロック図である。

【図２２】

中央サーバのハードウェア構成を示すブロック図である。

【図２３】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである

。

【図２４】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図２５】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図２６】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図２７】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図２８】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図２９】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャートである。

【図３０】

インストールされた消去用ソフトウェアの処理内容を示すフローチャートである。

【図３１】

実施の形態５に係る携帯電話機のハードウェア構成を示すブロック図である。

【図３２】

実施の形態６に係る携帯電話機のハードウェア構成を示すブロック図である。

【図３３】

実施の形態６に係る中央サーバのハードウェア構成を示すブロック図である。

【図３４】

実施の形態６に係る認証処理の手順を示すフローチャートである。

【図３５】

実施の形態６に係る認証処理の手順を示すフローチャートである。

【図３６】

実施の形態６に係る認証処理の手順を示すフローチャートである。

【図３７】

実施の形態６に係る認証処理の手順を示すフローチャートである。

【符号の説明】

１	携帯電話機（情報処理装置）
１１２	指紋取得部
２	中央サーバ（第１認証装置）
３	認証機関サーバ（第２認証装置）
４	Ｗｅｂサーバ（店舗コンピュータ）
Ｎ	インターネット（通信網）
１１０	携帯電話機エンジン部
１５	ＲＯＭ
１６	アンテナ部
１３	入力部
１１３	電源部
１９	外部接続端子
５	セキュリティチップ（安全性判断装置）
５５２	指紋情報ファイル
５５１	環境情報ファイル
５５３	電子証明書ファイル
５５４	個人鍵ファイル
２４	表示部
２３	入力部
２５１	環境情報データベース（環境情報ＤＢ）
１ａ	記録媒体

１１４　　主電源部（主電力供給手段）

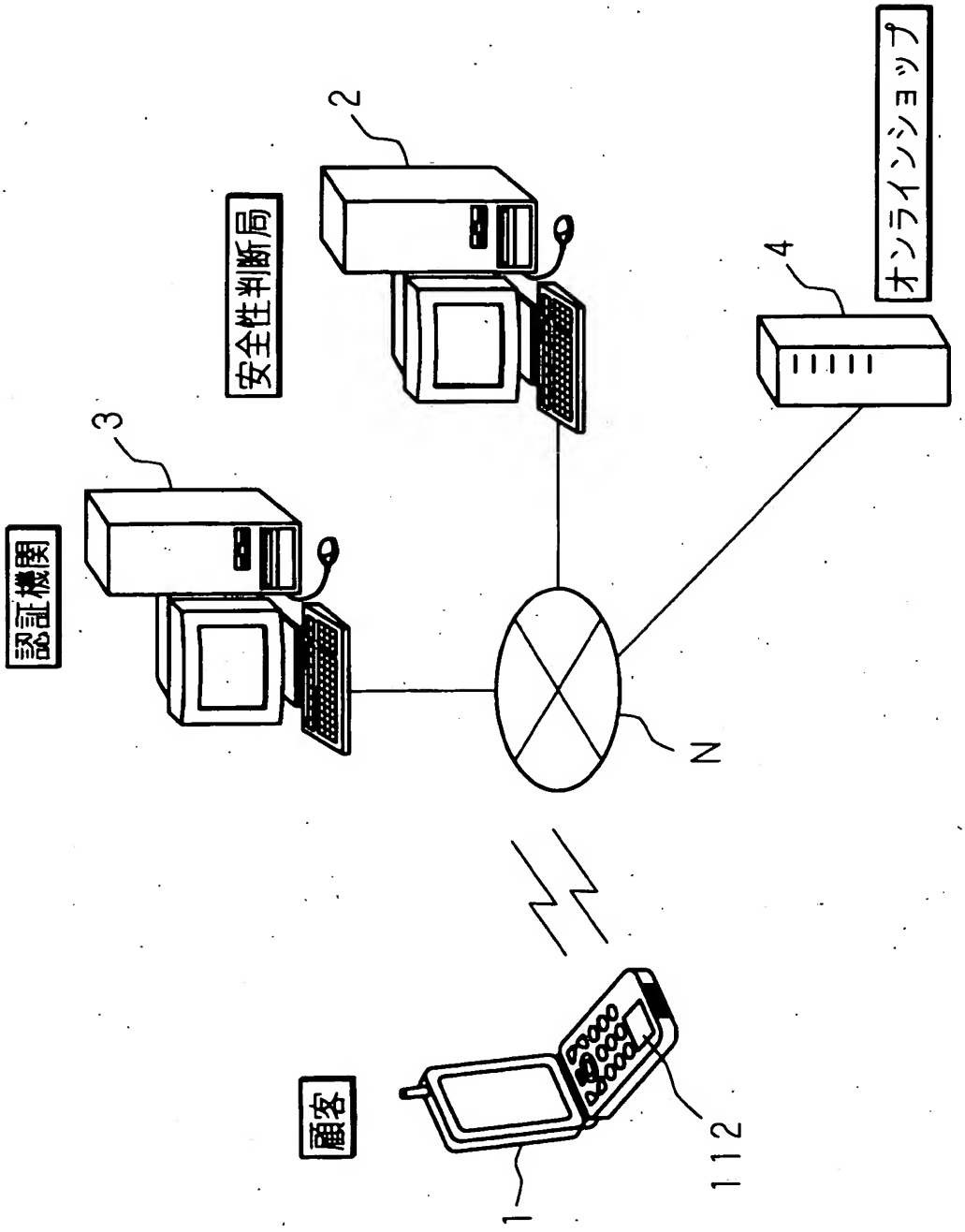
１１５　　副電源部（副電力供給手段）

１１６　　第２ＲＯＭ（蓄積手段）

【書類名】　図面

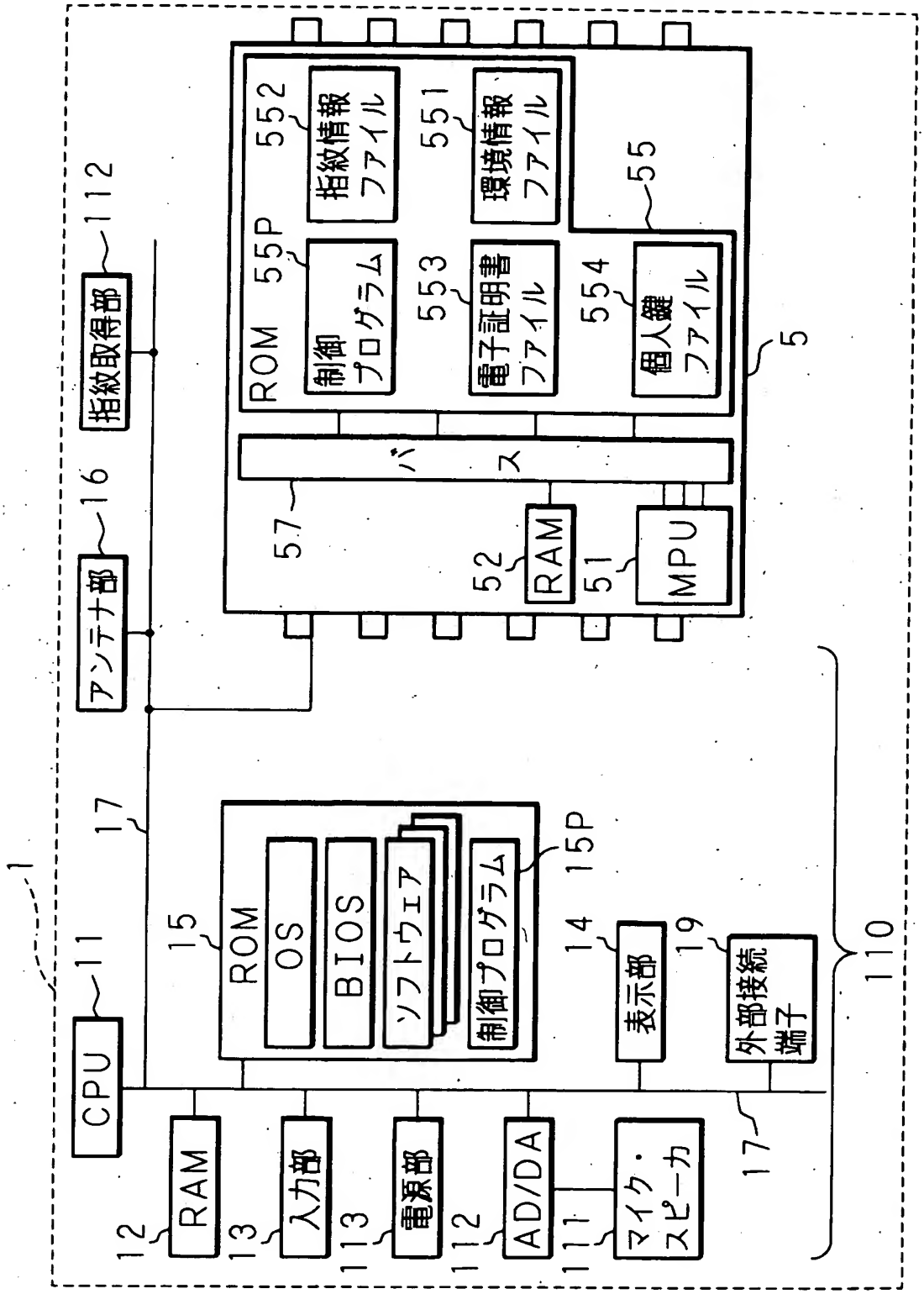
【図１】

本発明に係る安全性判断システムの概要を示す模式図



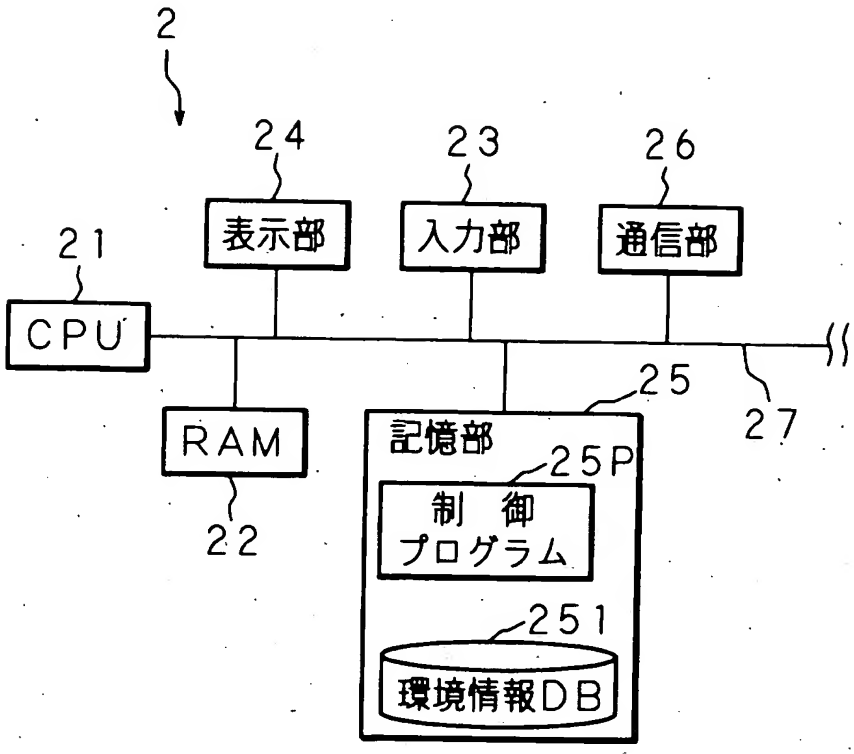
【図２】

携帯電話機のハードウェア構成を示すブロック図



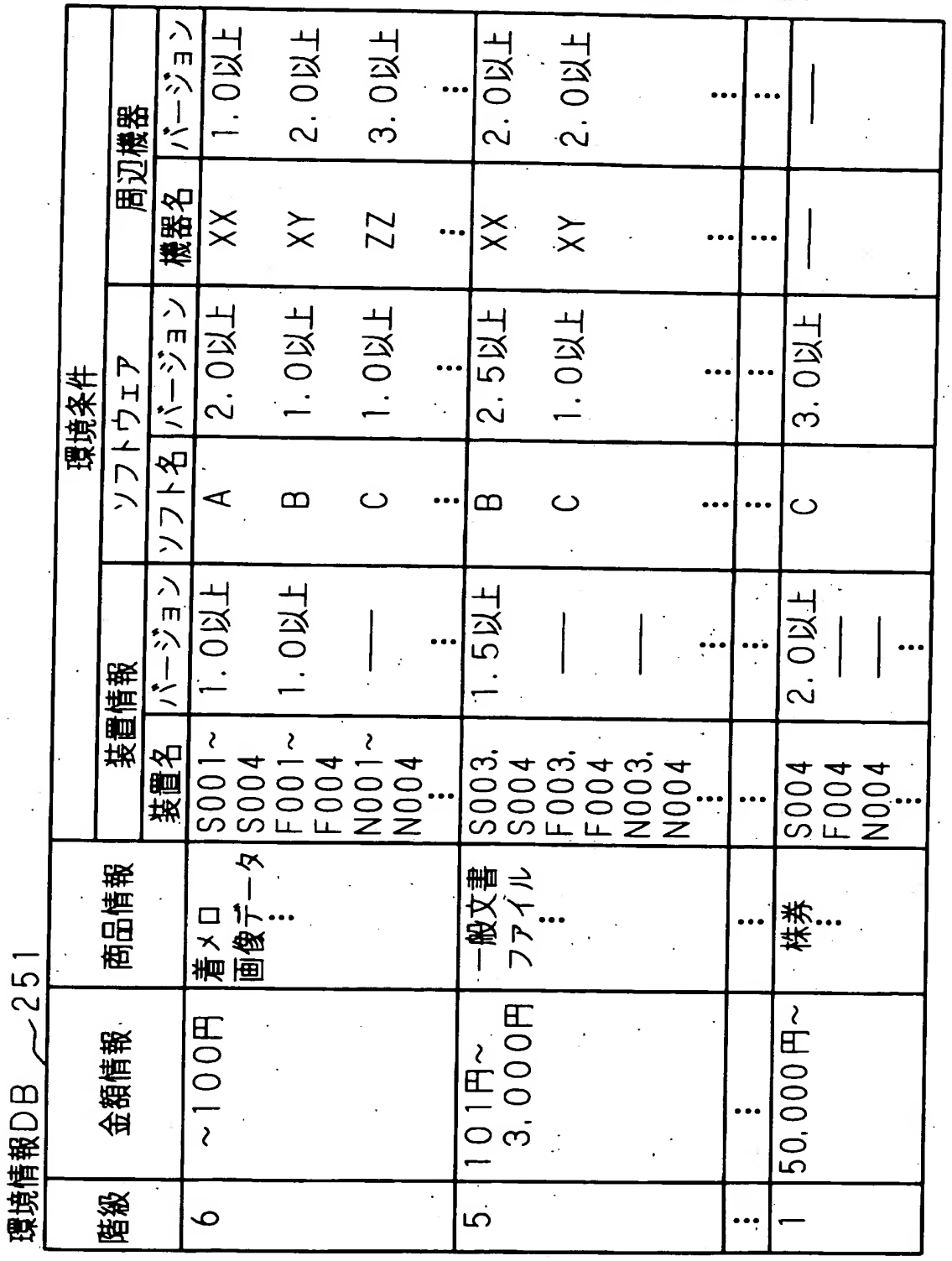
【図３】

中央サーバのハードウェア構成を示すブロック図

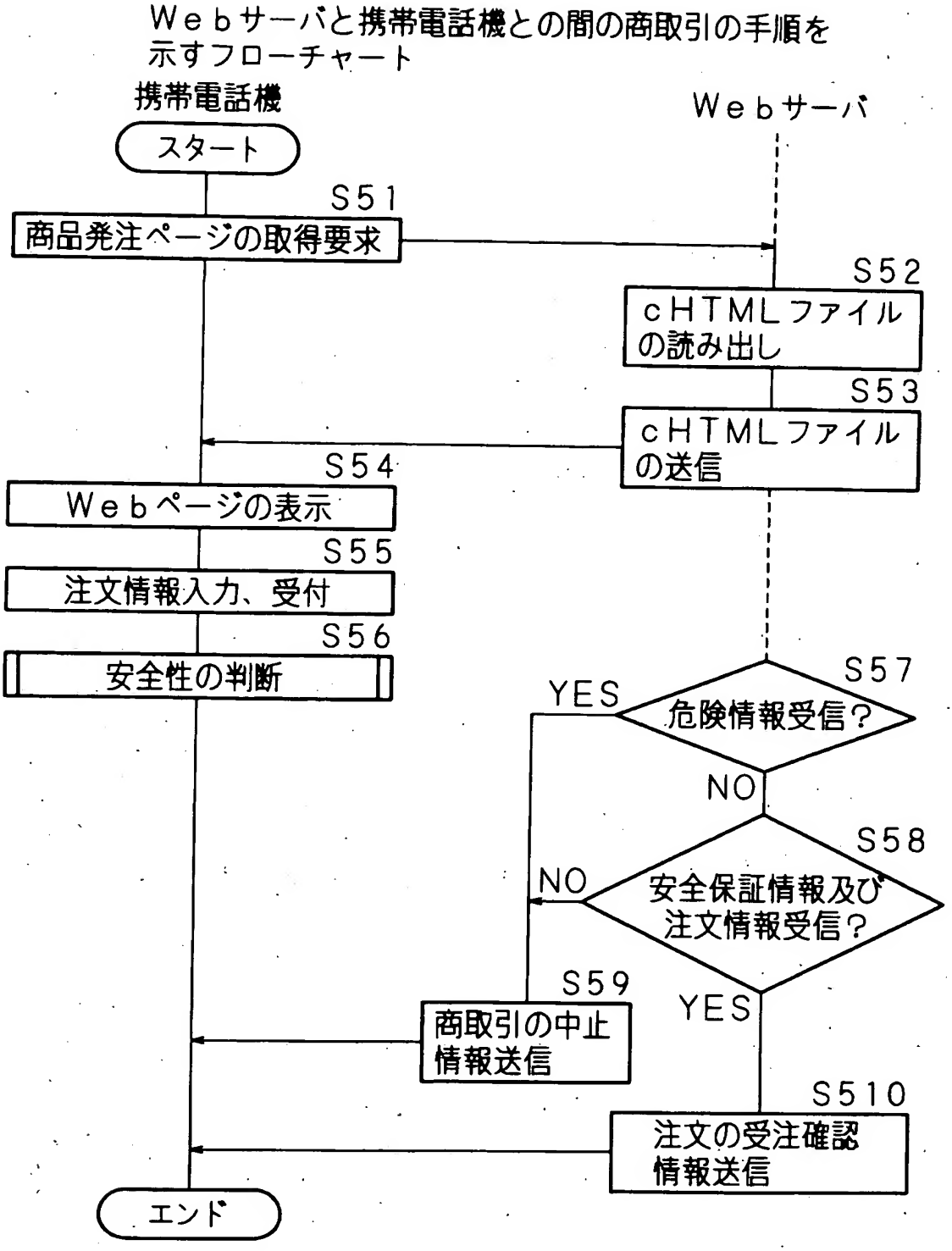


【図４】

環境情報ＤＢのレコードレイアウトを示す説明図

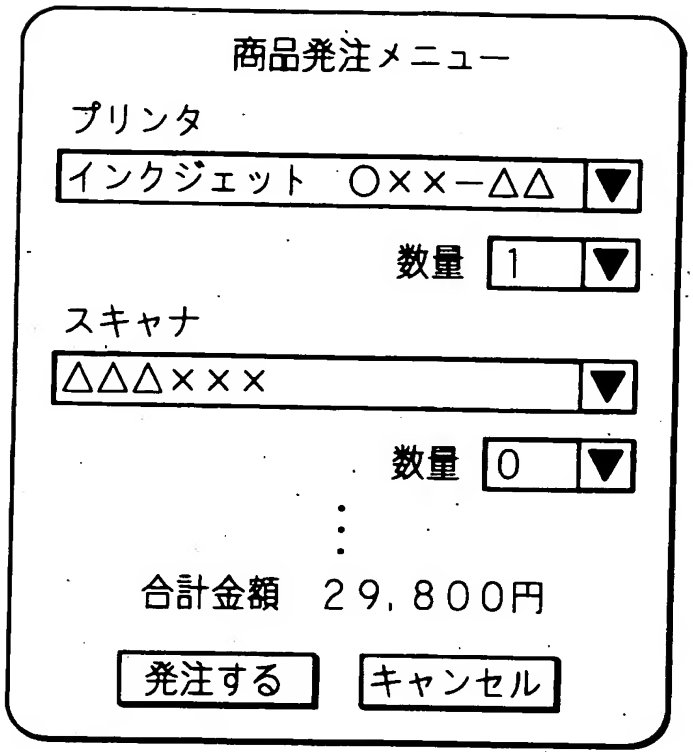


【図５】


Ｗｅｂサーバと携帯電話機との間の商取引の手順を示すフローチャート
携帯電話機
Ｗｅｂサーバ
スタート
S51
商品発注ページの取得要求
S52
ｃＨＴＭＬファイルの読み出し
S53
ｃＨＴＭＬファイルの送信
S54
Ｗｅｂページの表示
S55
注文情報入力、受付
S56
安全性の判断
S57
危険情報受信？
YES
NO
S58
安全保証情報及び注文情報受信？
NO
YES
S59
商取引の中止情報送信
S510
注文の受注確認情報送信
エンド

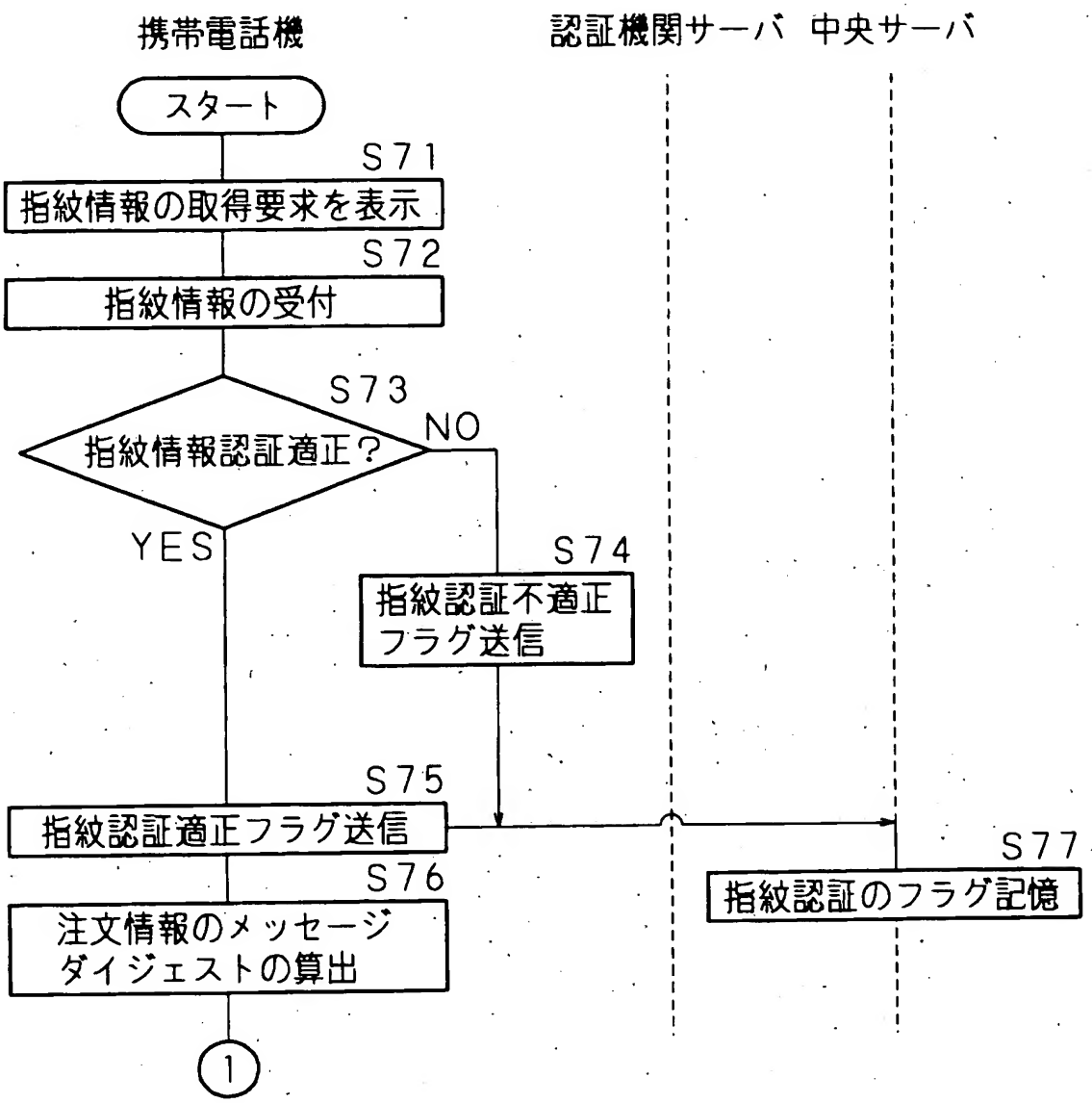
【図６】

Ｗｅｂページのイメージを示す説明図

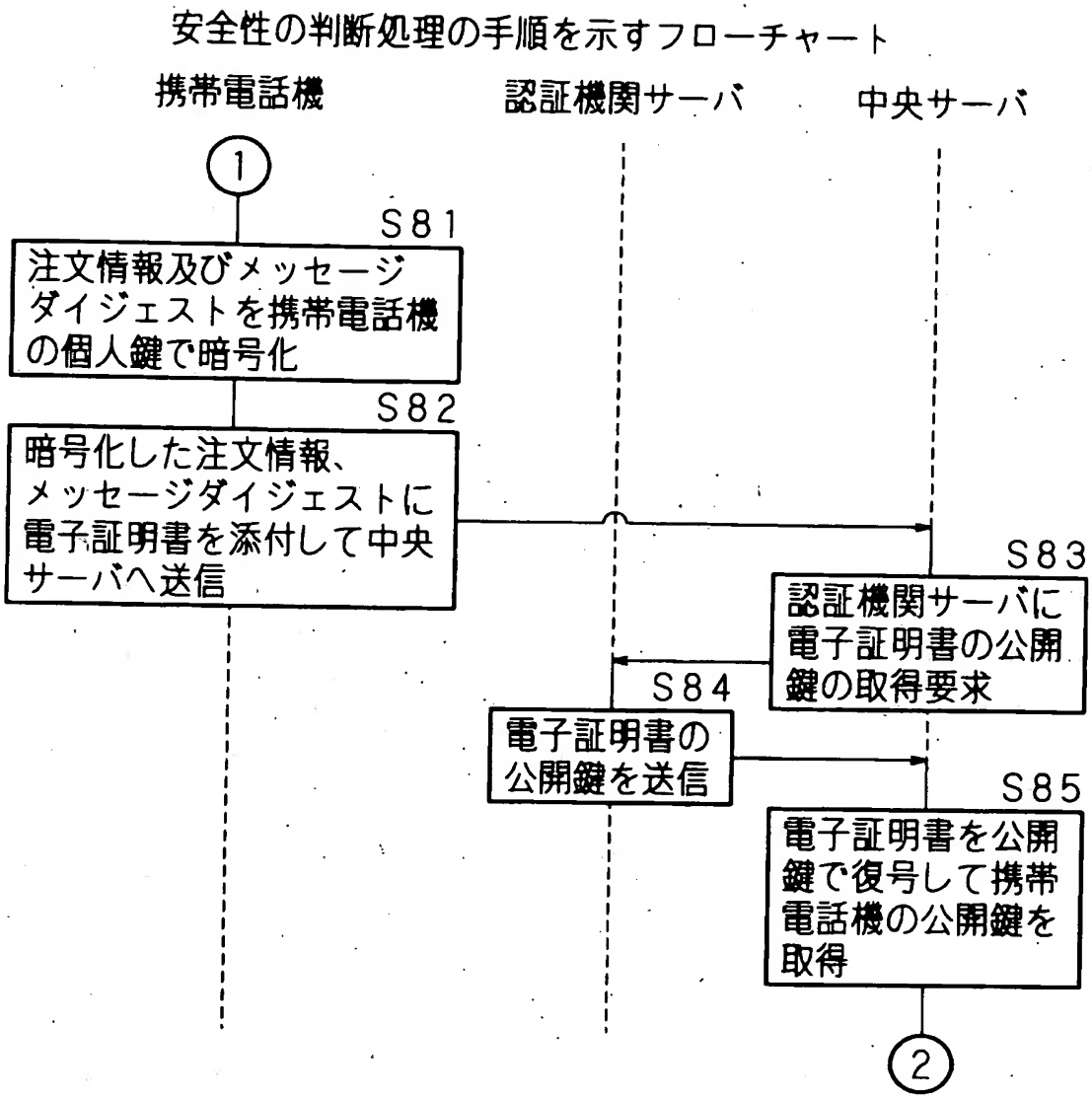


【図７】

安全性の判断処理の手順を示すフローチャート

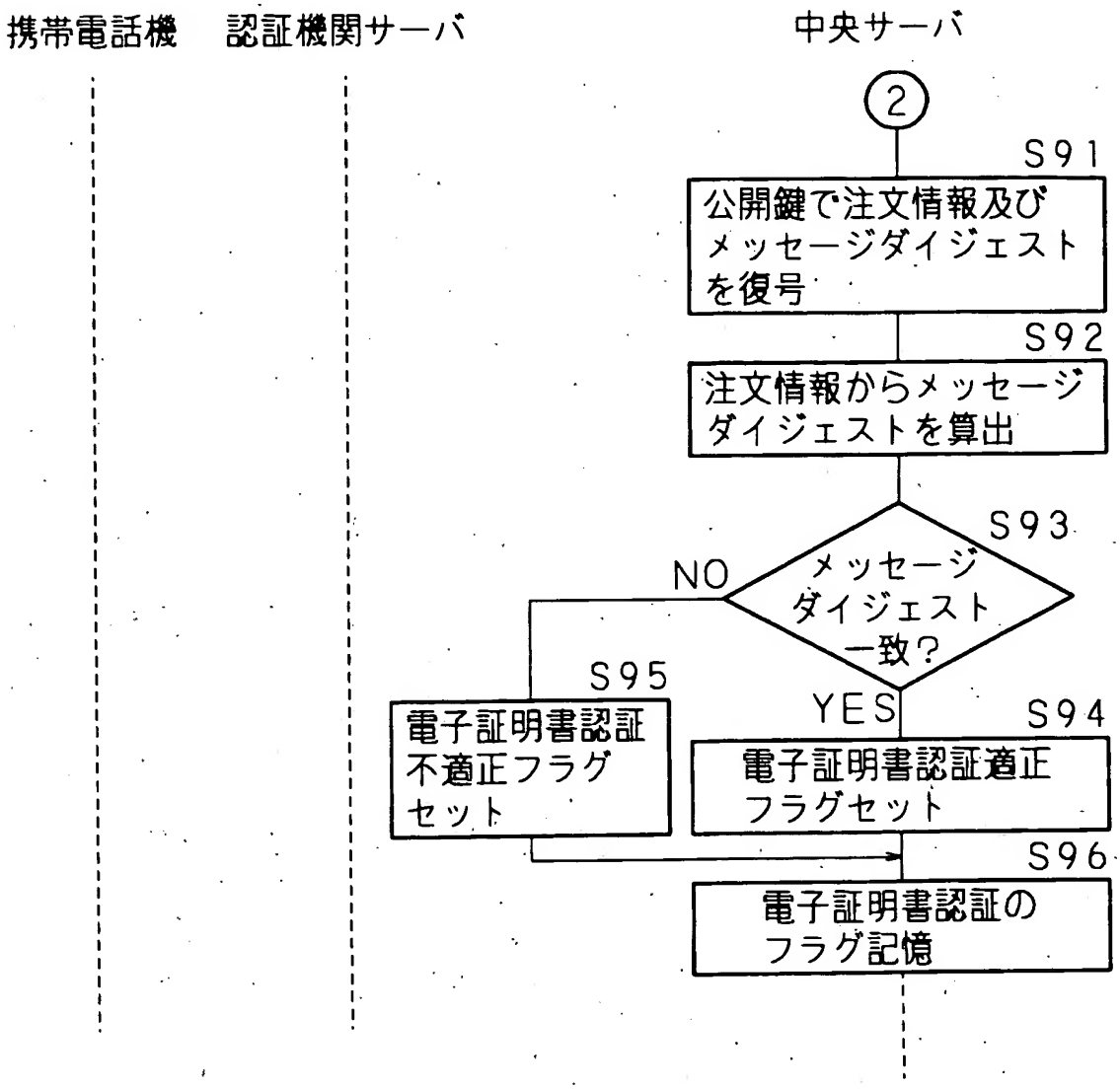


【図８】

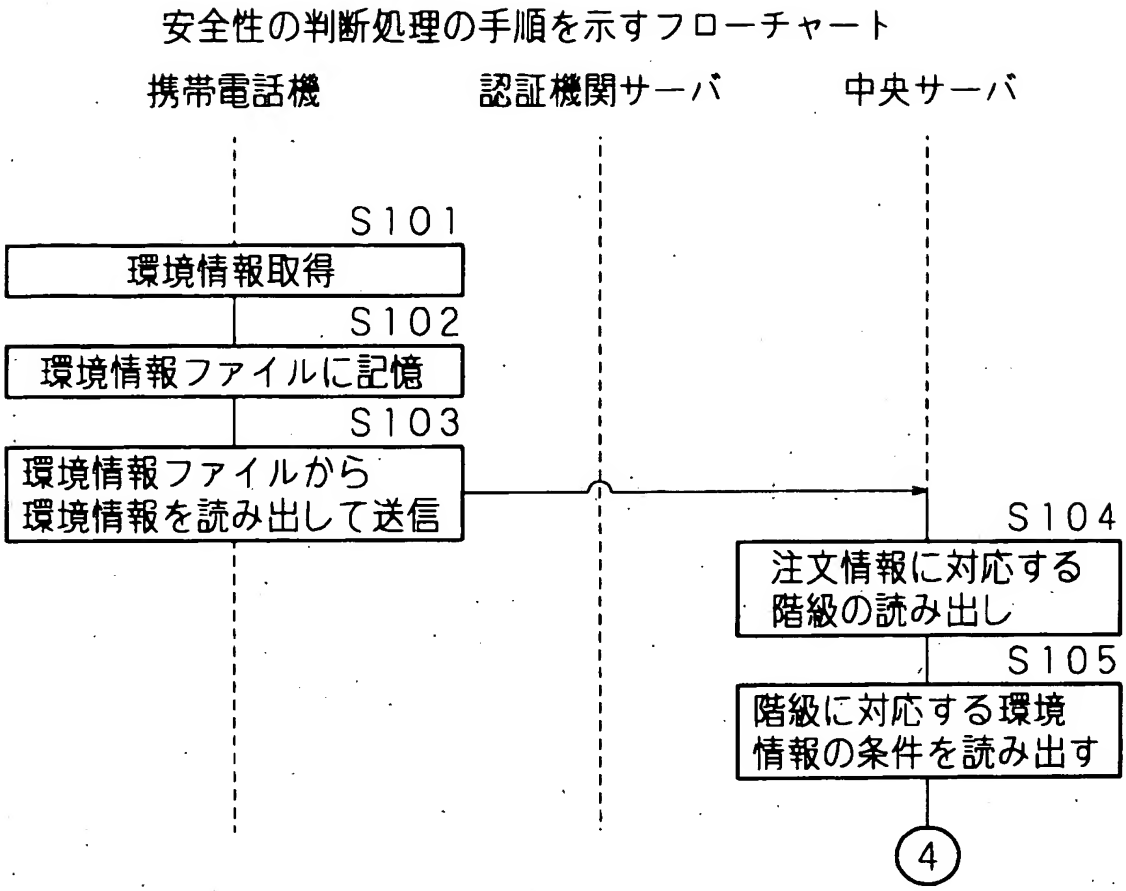

安全性の判断処理の手順を示すフローチャート
携帯電話機
認証機関サーバ
中央サーバ
①
S81
注文情報及びメッセージダイジェストを携帯電話機の個人鍵で暗号化
S82
暗号化した注文情報、メッセージダイジェストに電子証明書を添付して中央サーバへ送信
S83
認証機関サーバに電子証明書の公開鍵の取得要求
S84
電子証明書の公開鍵を送信
S85
電子証明書を公開鍵で復号して携帯電話機の公開鍵を取得
②

【図９】

安全性の判断処理の手順を示すフローチャート

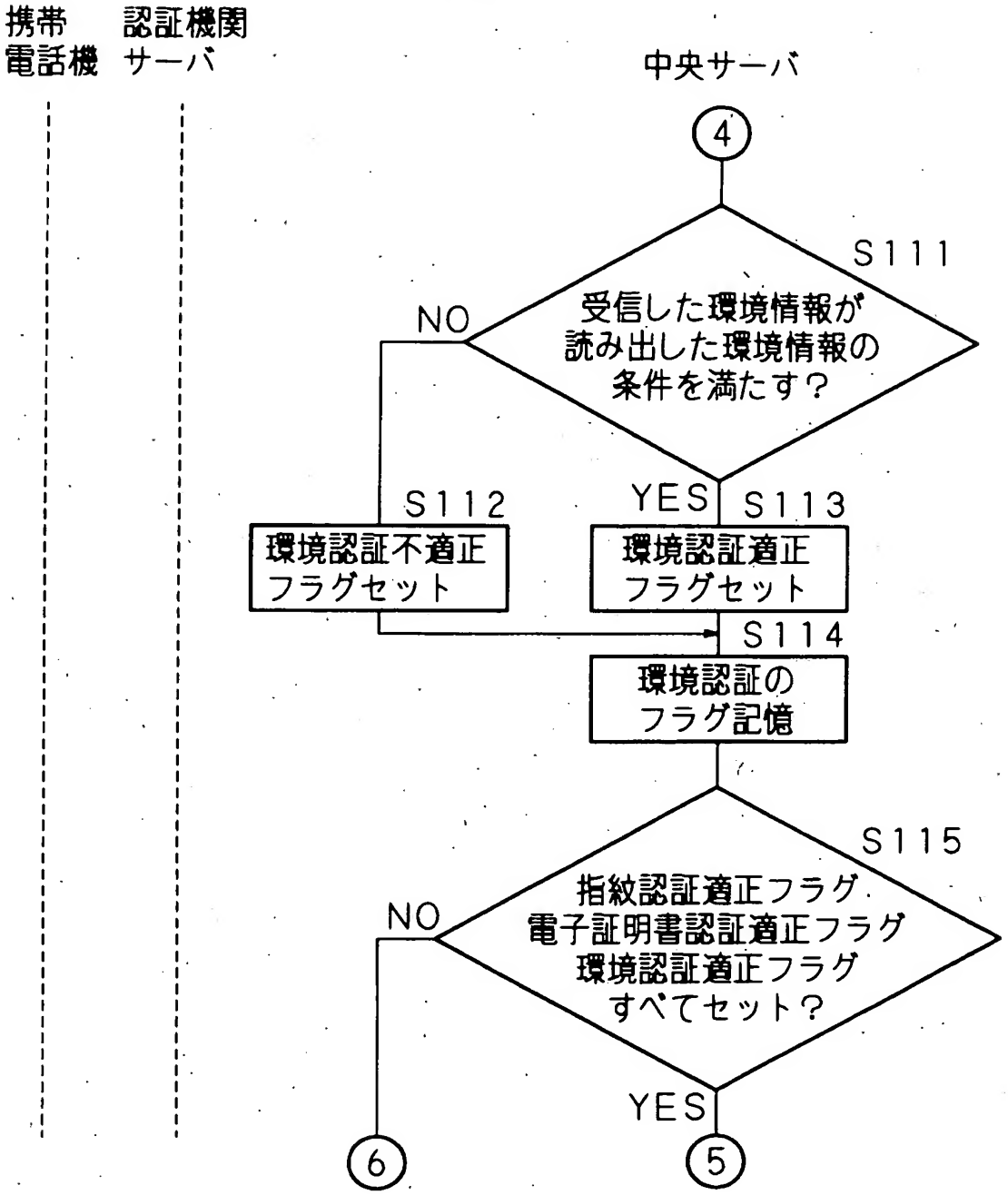


【図１０】


安全性の判断処理の手順を示すフローチャート
携帯電話機
認証機関サーバ
中央サーバ
S101
環境情報取得
S102
環境情報ファイルに記憶
S103
環境情報ファイルから
環境情報を読み出して送信
S104
注文情報に対応する
階級の読み出し
S105
階級に対応する環境
情報の条件を読み出す
4

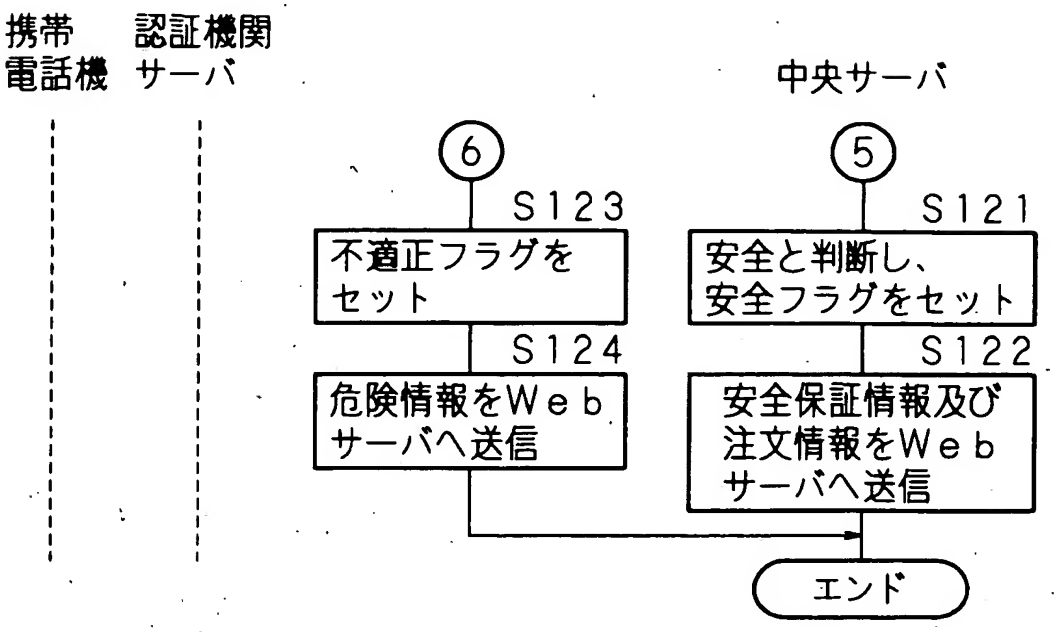
【図１１】

安全性の判断処理の手順を示すフローチャート



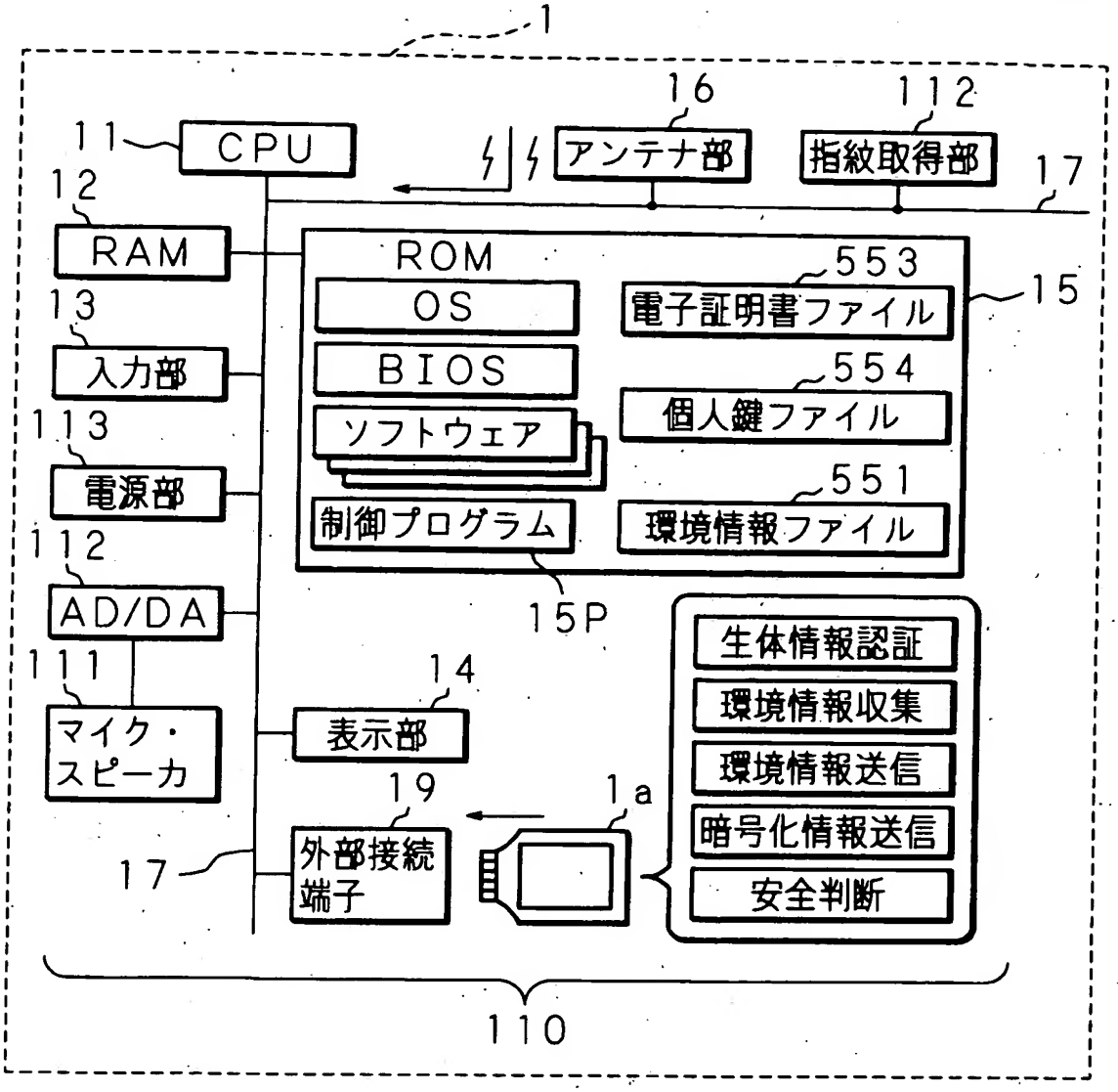
【図１２】

安全性の判断処理の手順を示すフローチャート



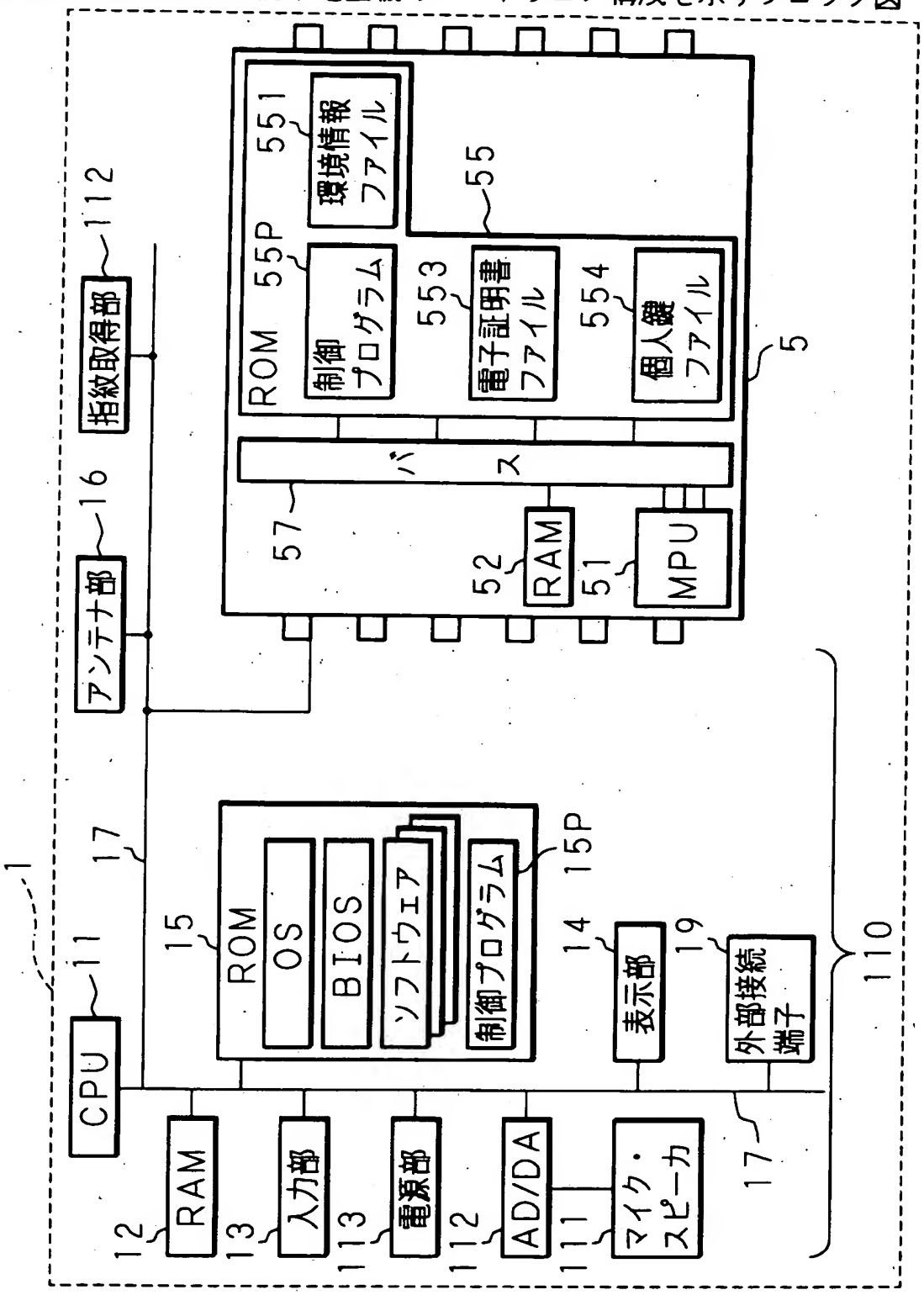
【図１３】

実施の形態２に係る携帯電話機のハードウェア構成を示すブロック図



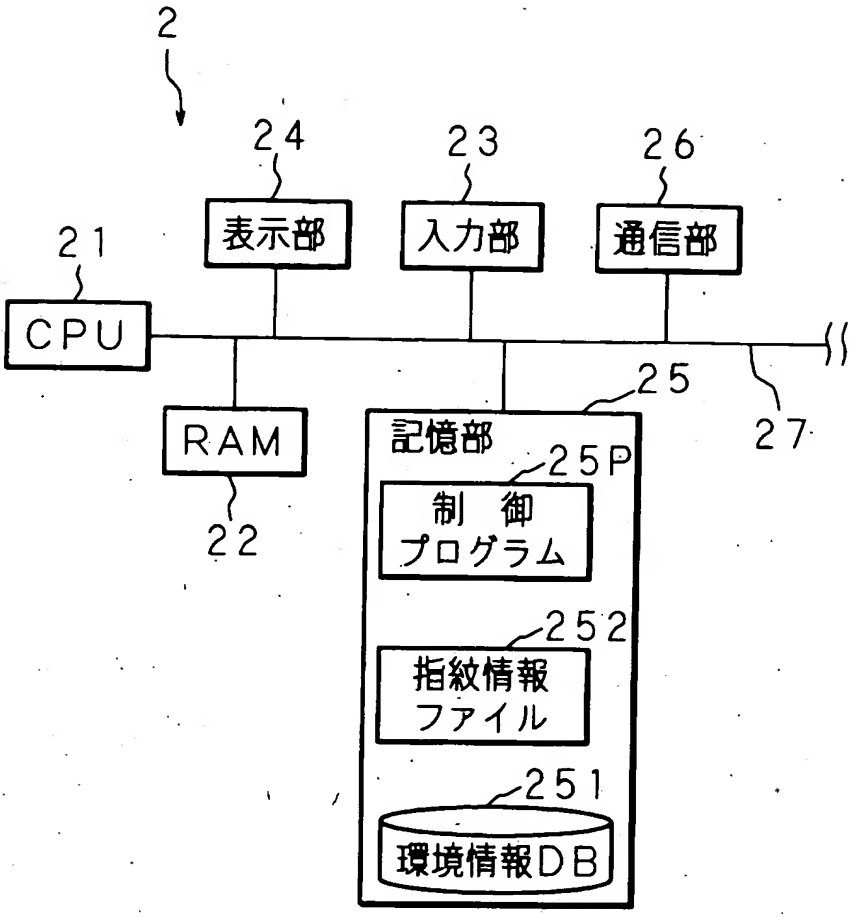
【図１４】

実施の形態３に係る携帯電話機のハードウェア構成を示すブロック図



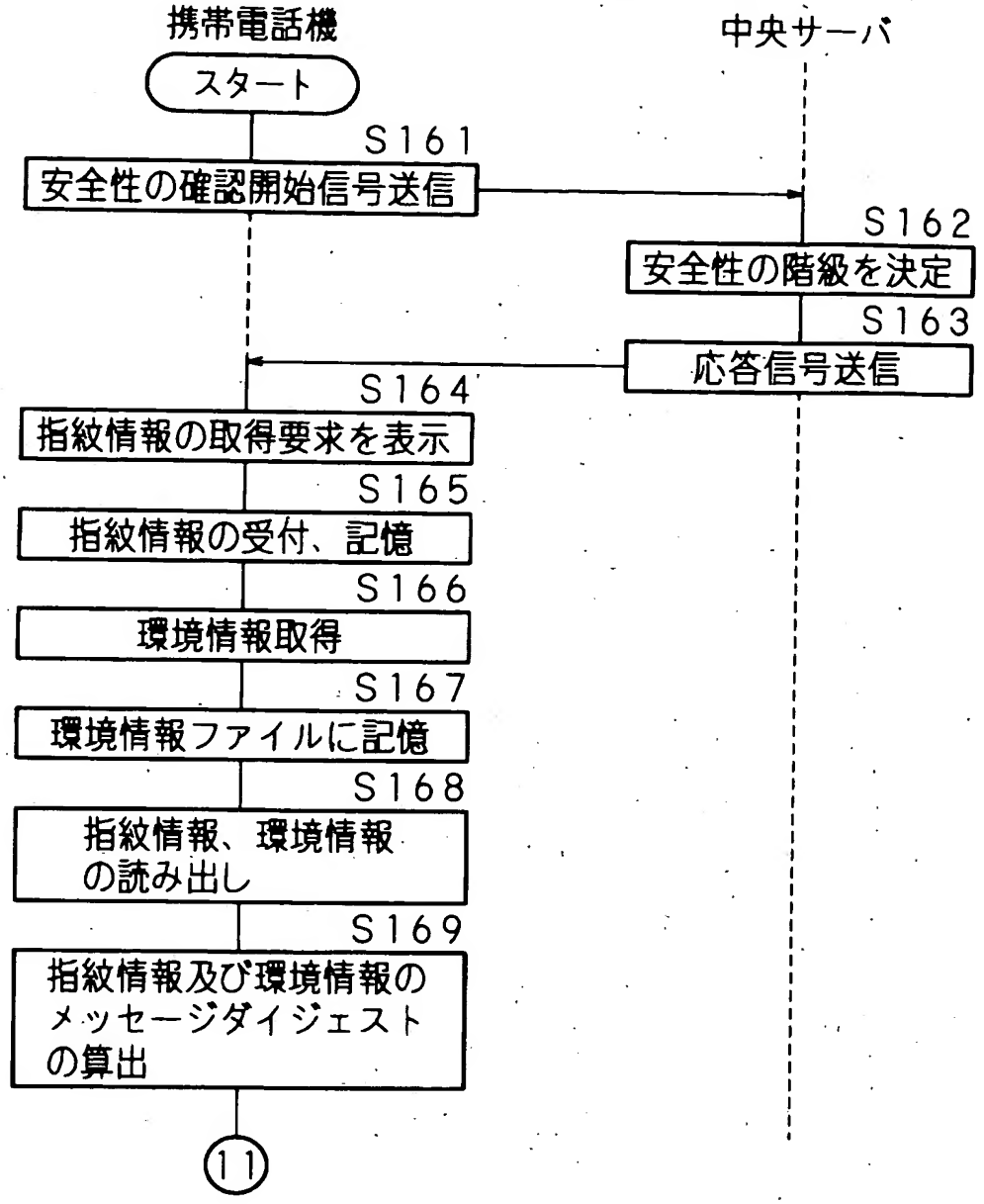
【図１５】

中央サーバのハードウェア構成を示すブロック図



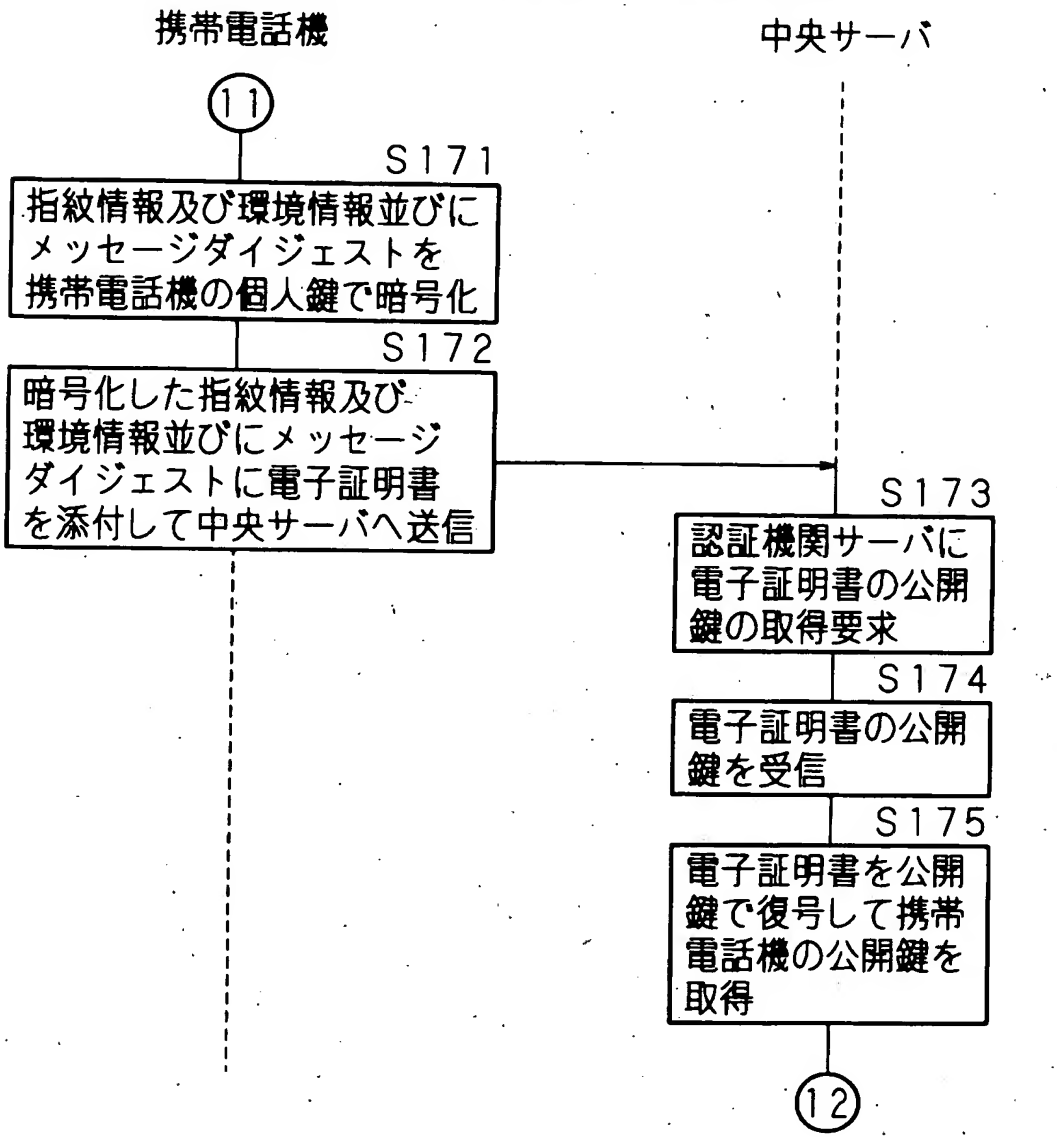
【図１６】

実施の形態３に係る安全性の判断処理の手順を示すフローチャート



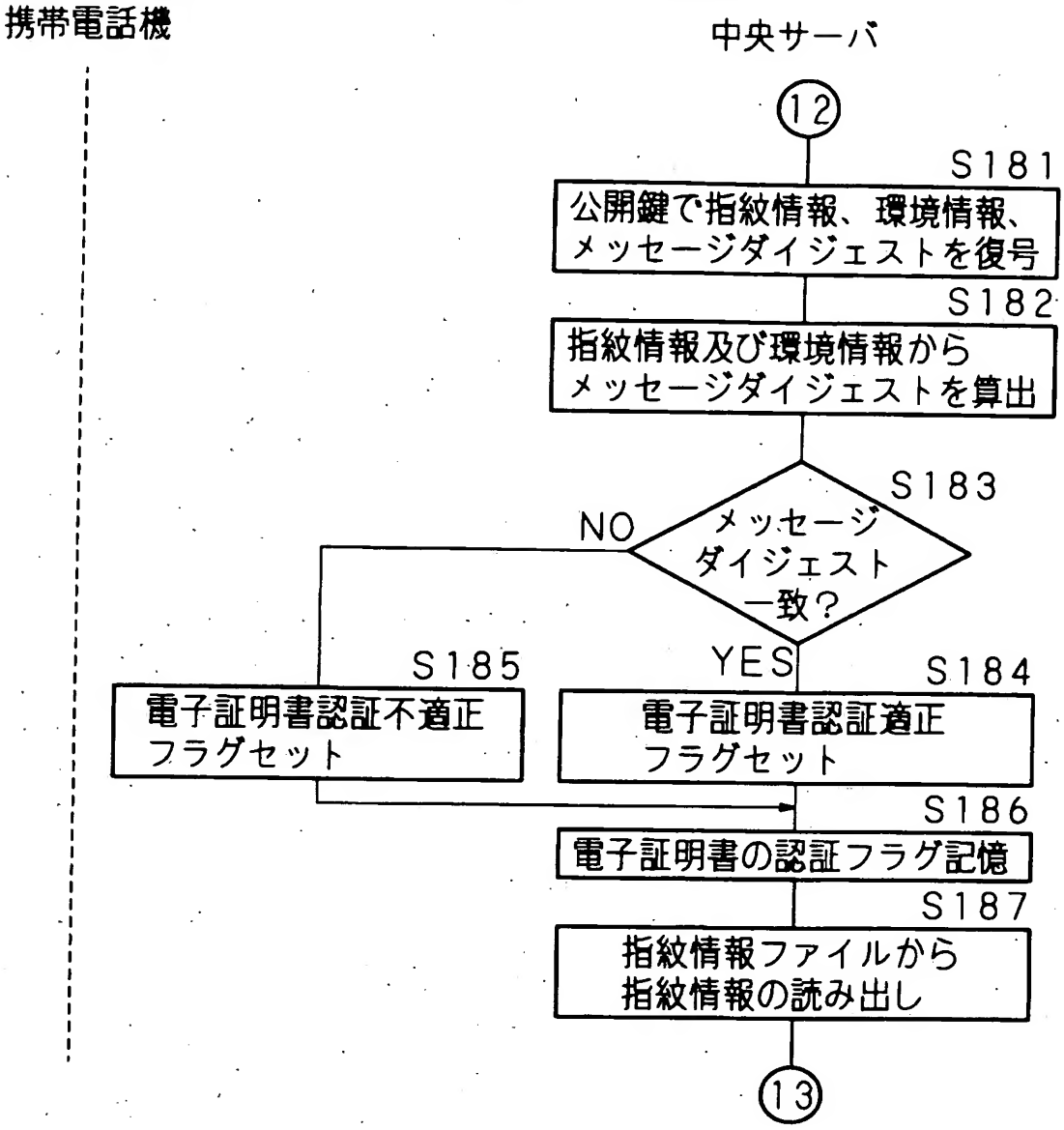
【図１７】

実施の形態３に係る安全性の判断処理の手順を示すフローチャート



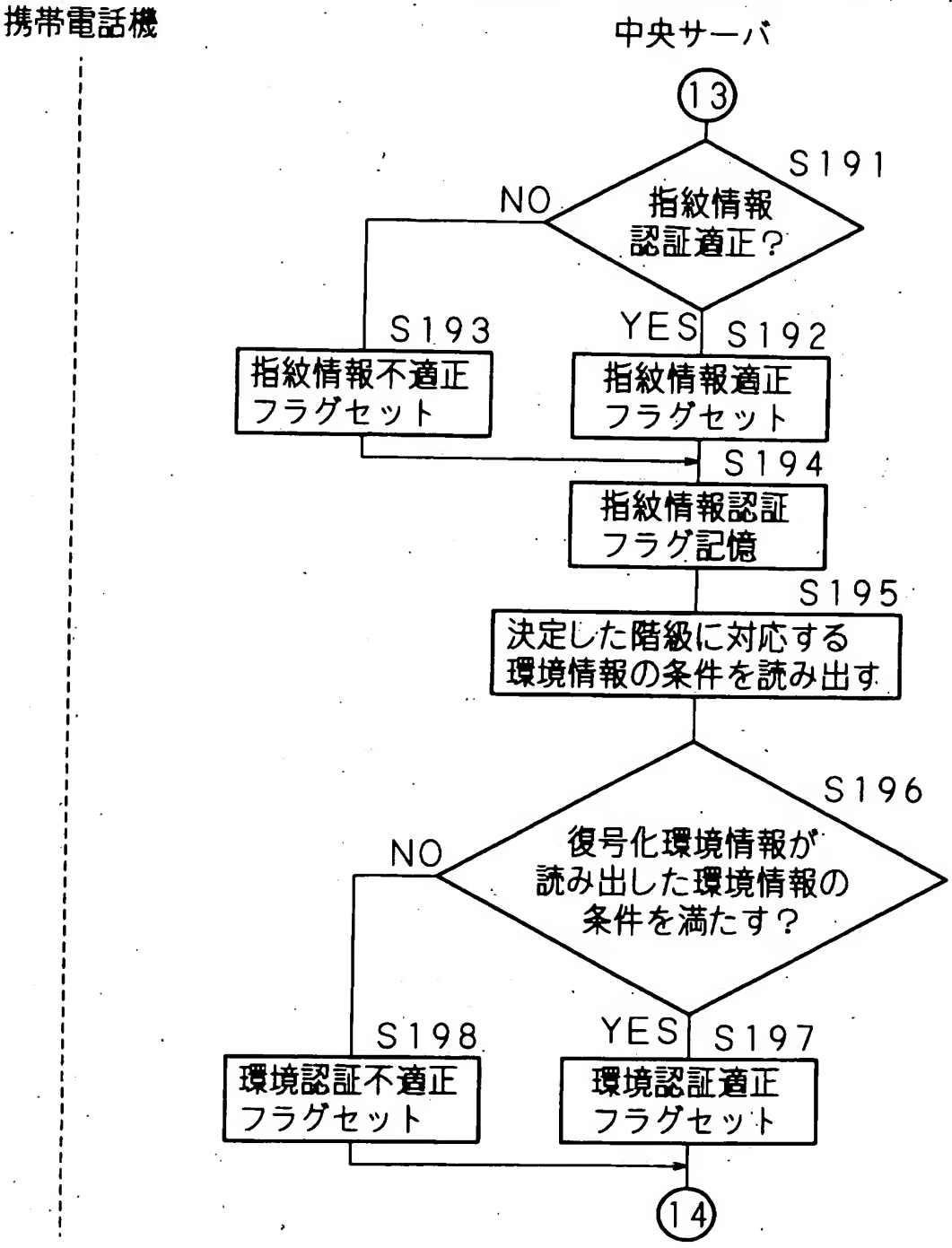
【図１８】

実施の形態３に係る安全性の判断処理の手順を示すフローチャート



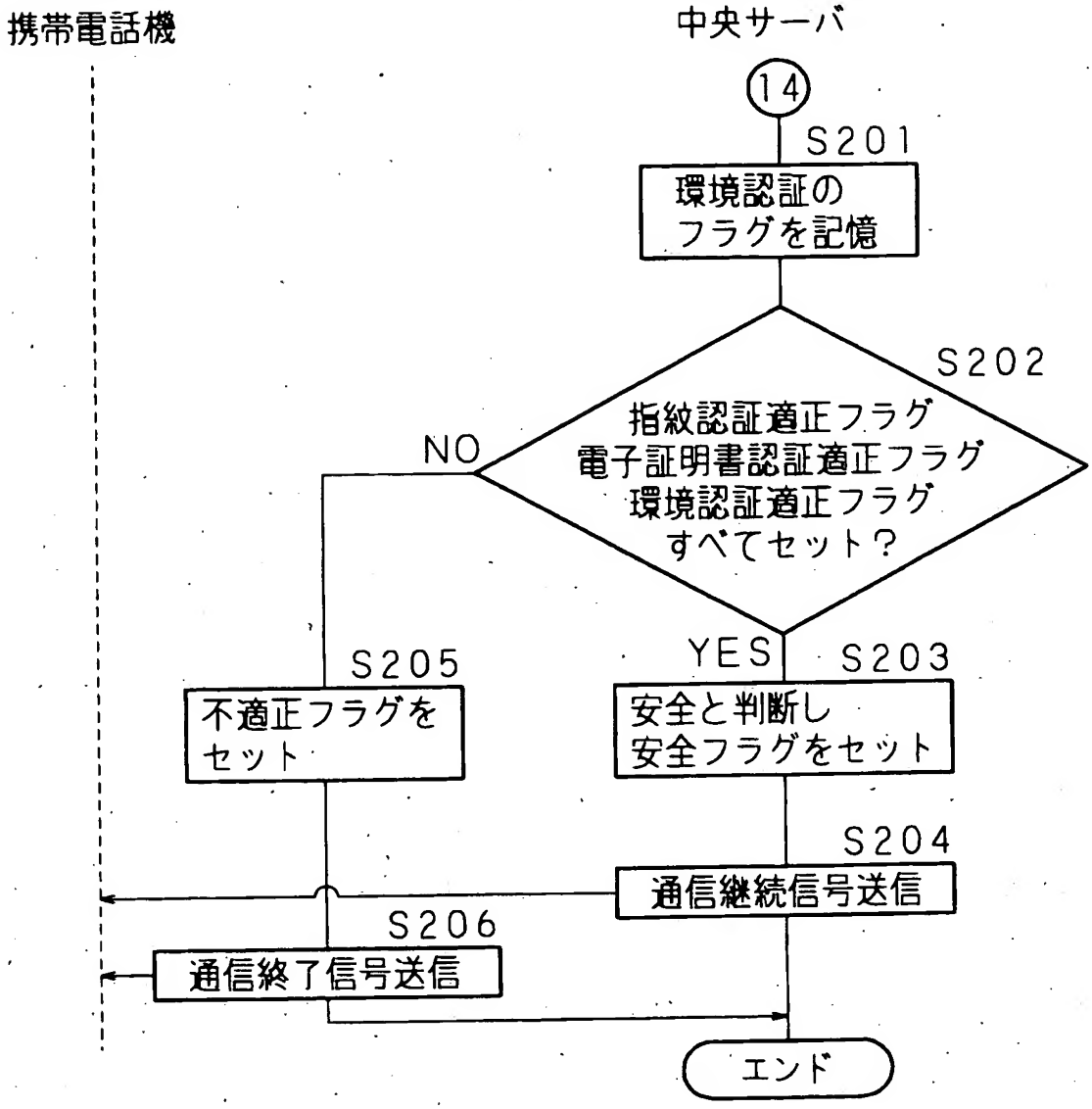
【図１９】

実施の形態３に係る安全性の判断処理の手順を示すフローチャート



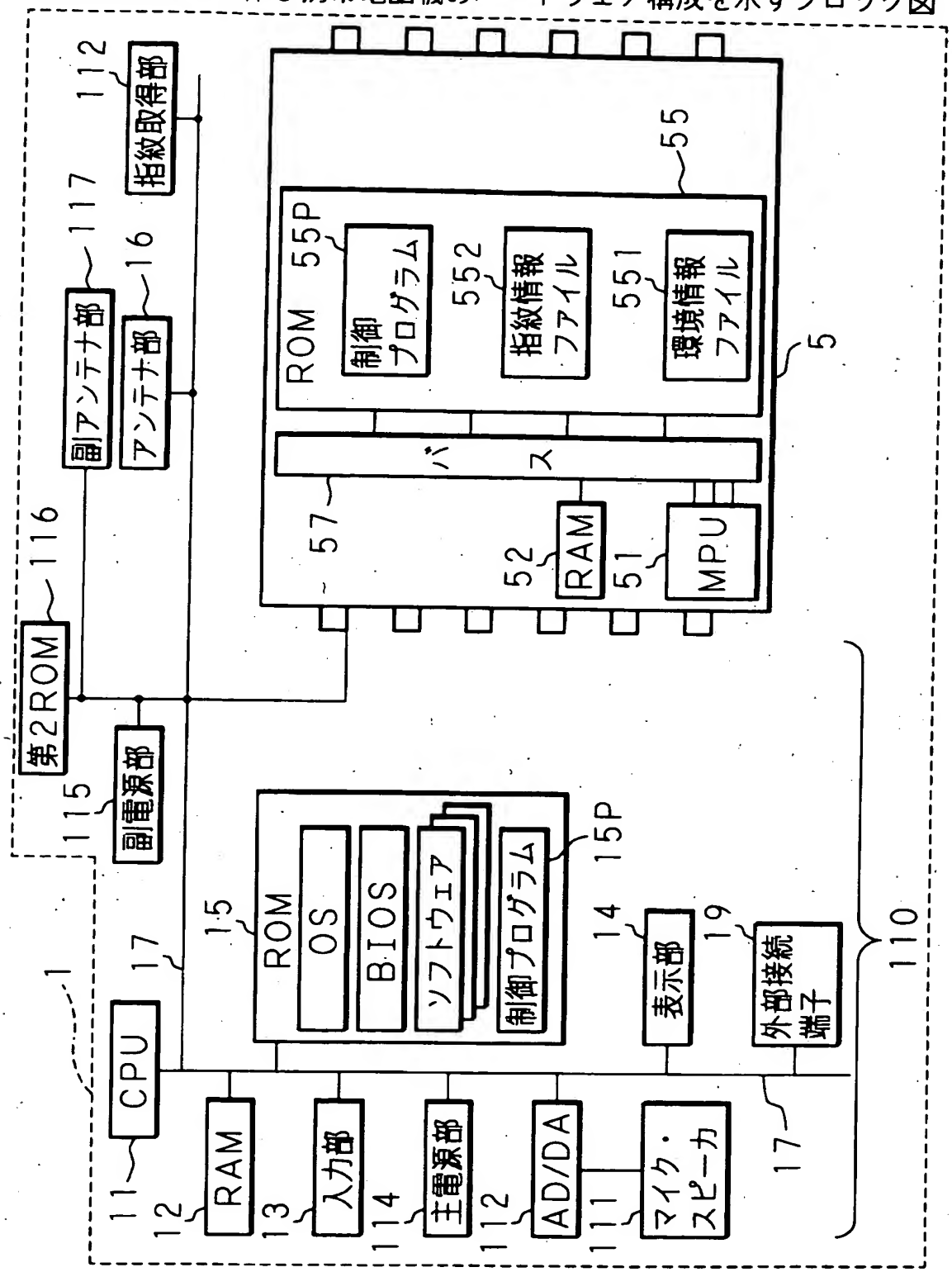
【図２０】

実施の形態３に係る安全性の判断処理の手順を示すフローチャート



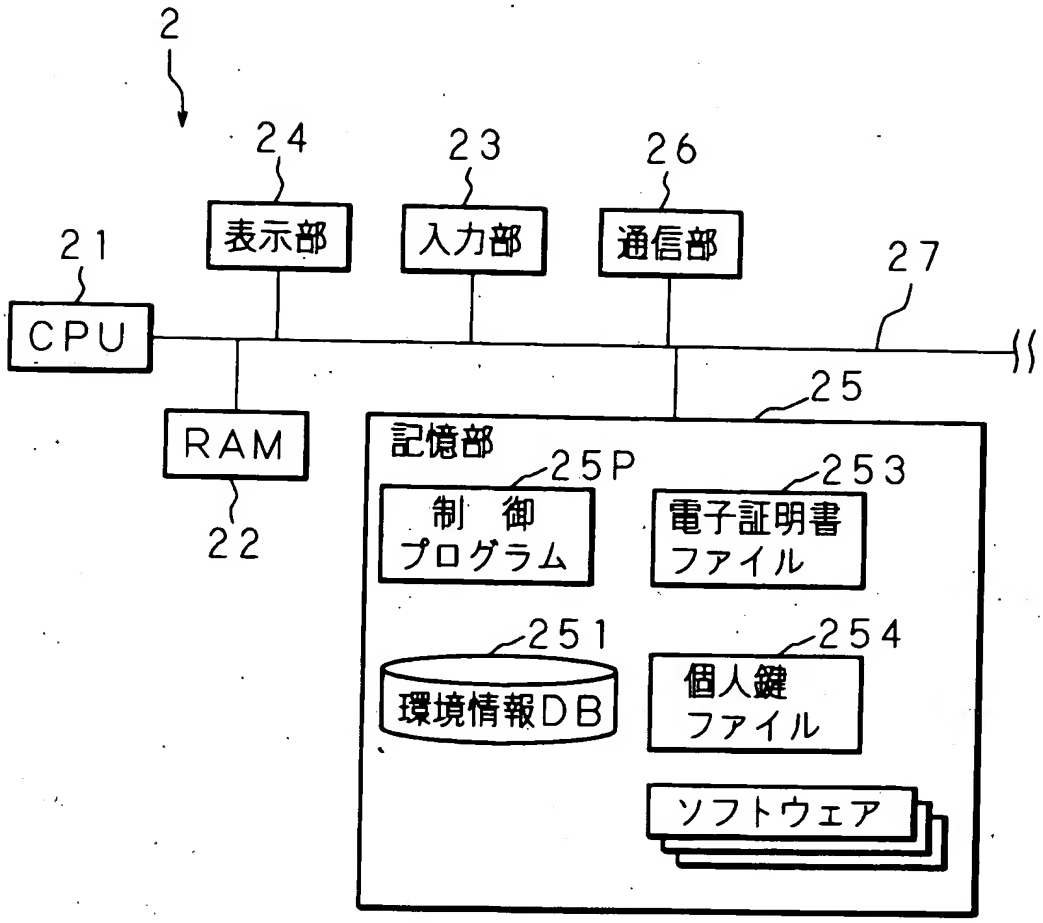
【図２１】

実施の形態４に係る携帯電話機のハードウェア構成を示すブロック図



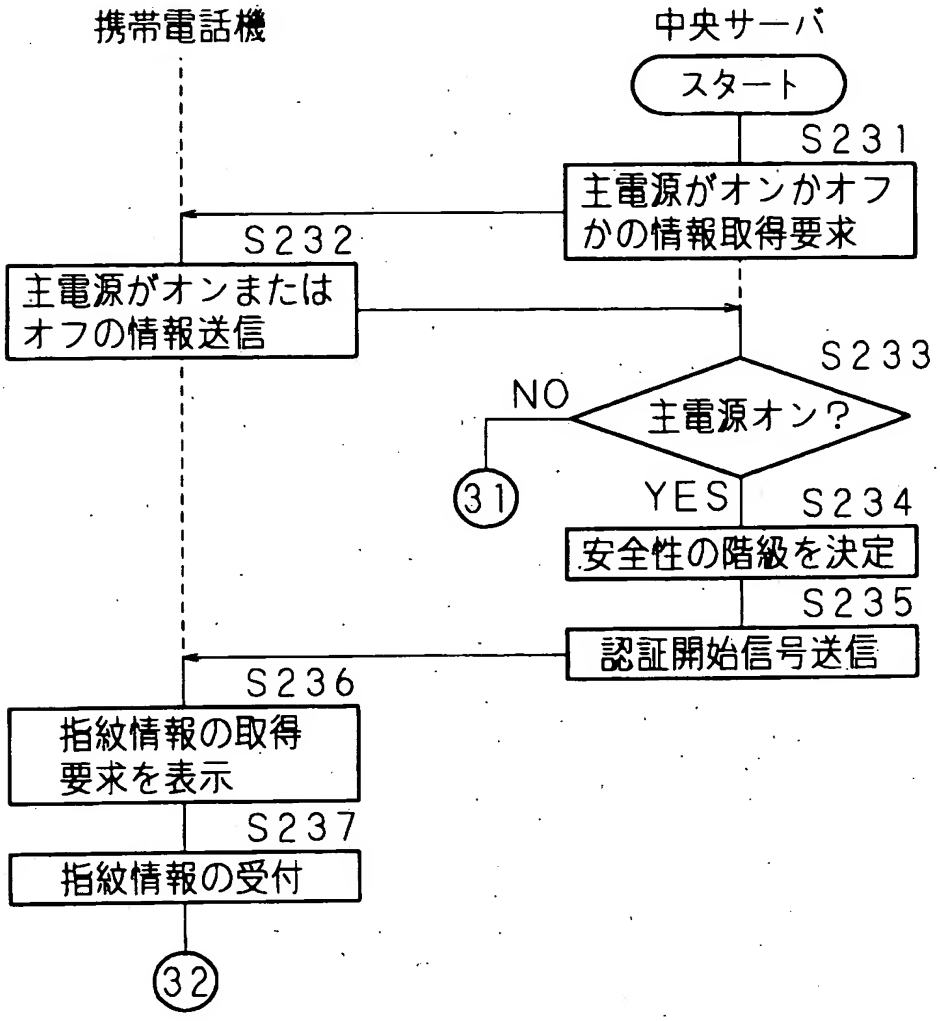
【図２２】

中央サーバのハードウェア構成を示すブロック図



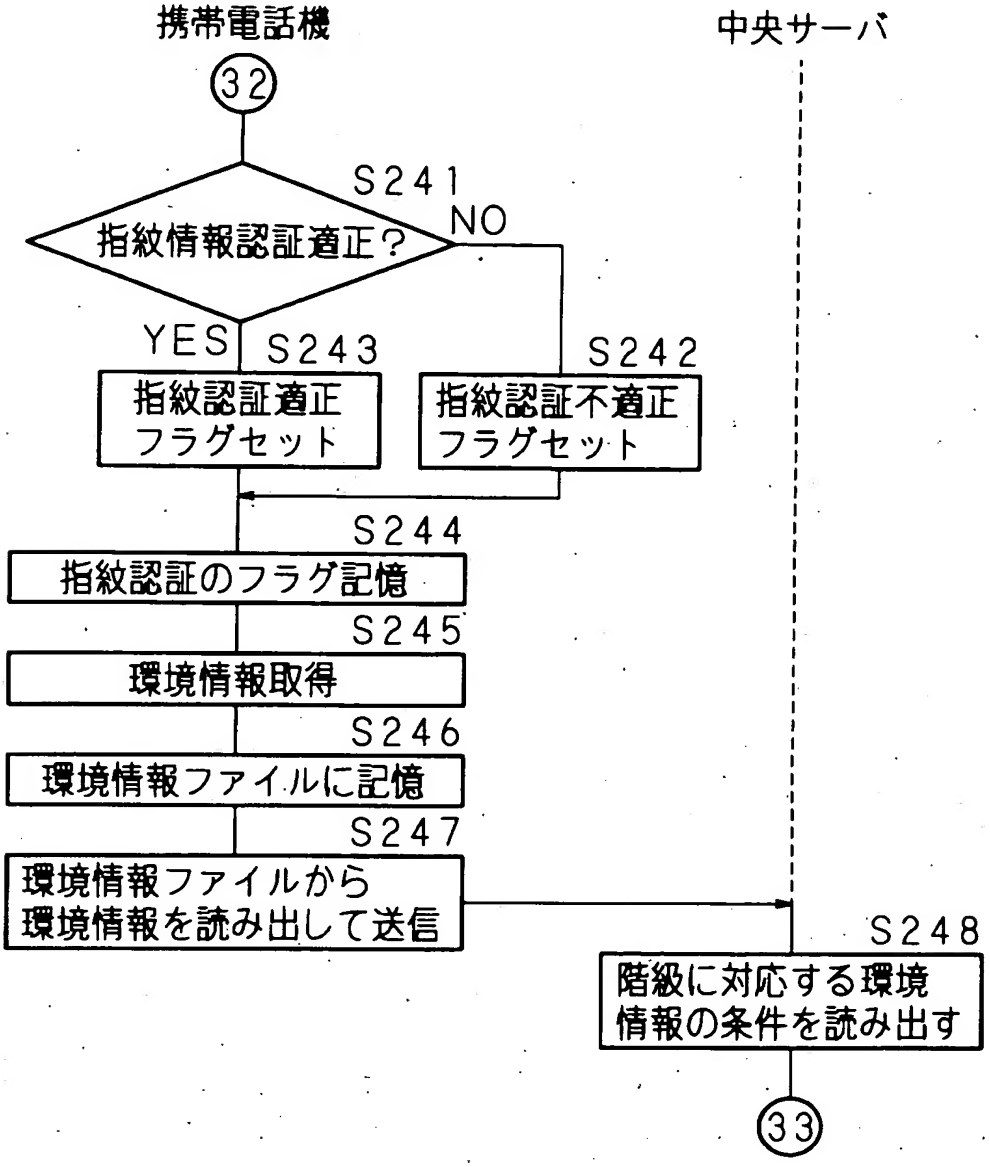
【図２３】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



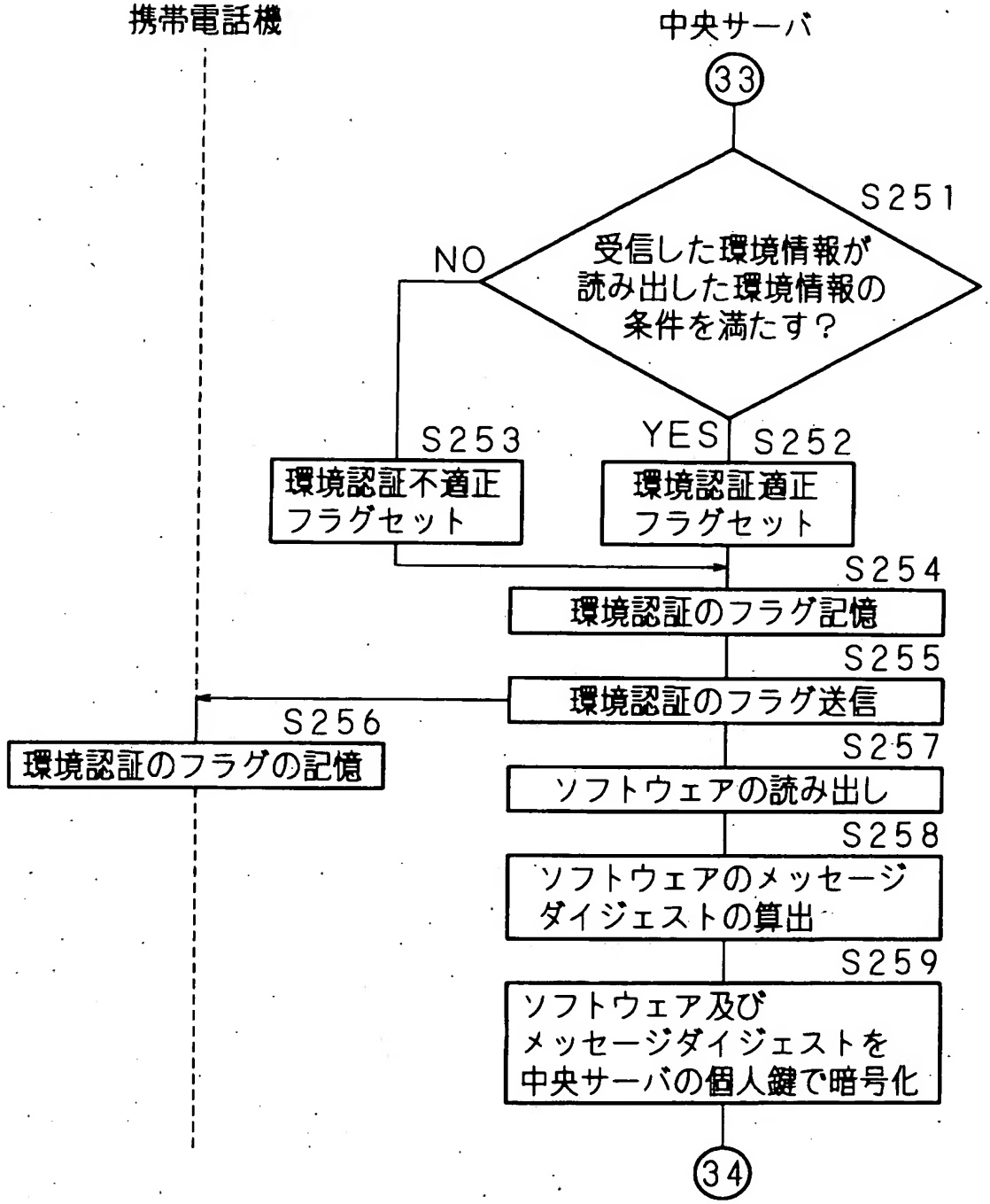
【図２４】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



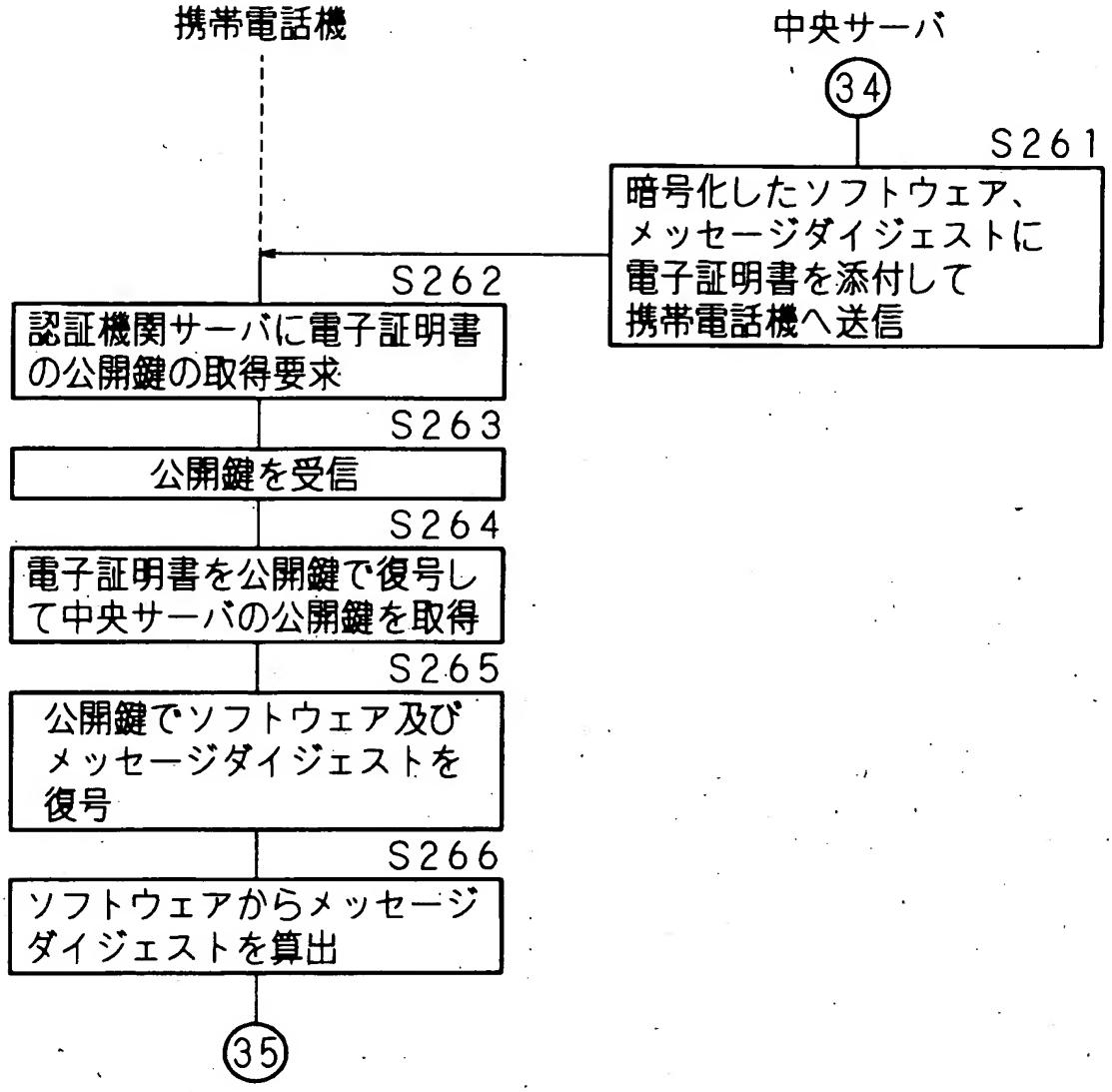
【図２５】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



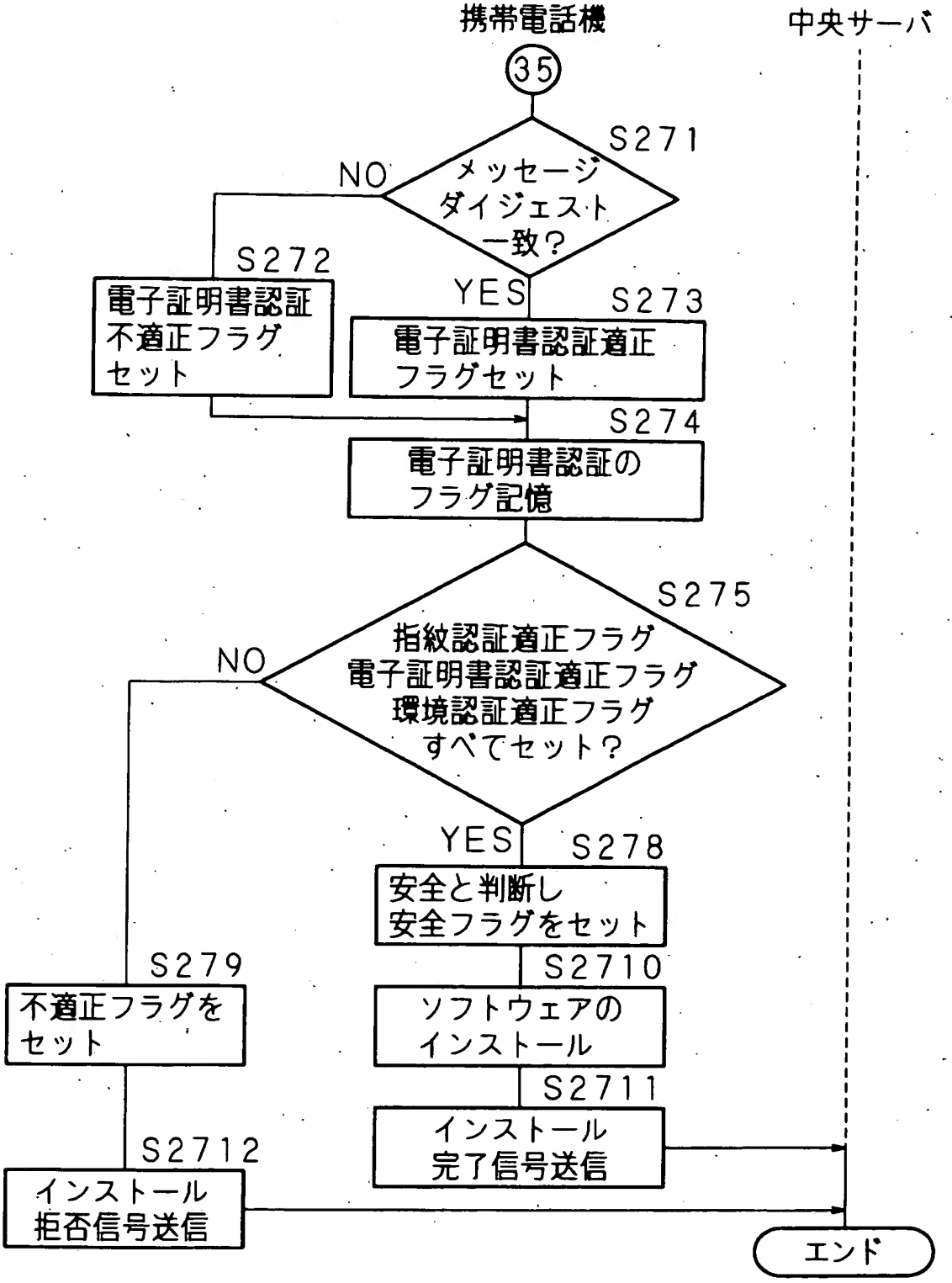
【図２６】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



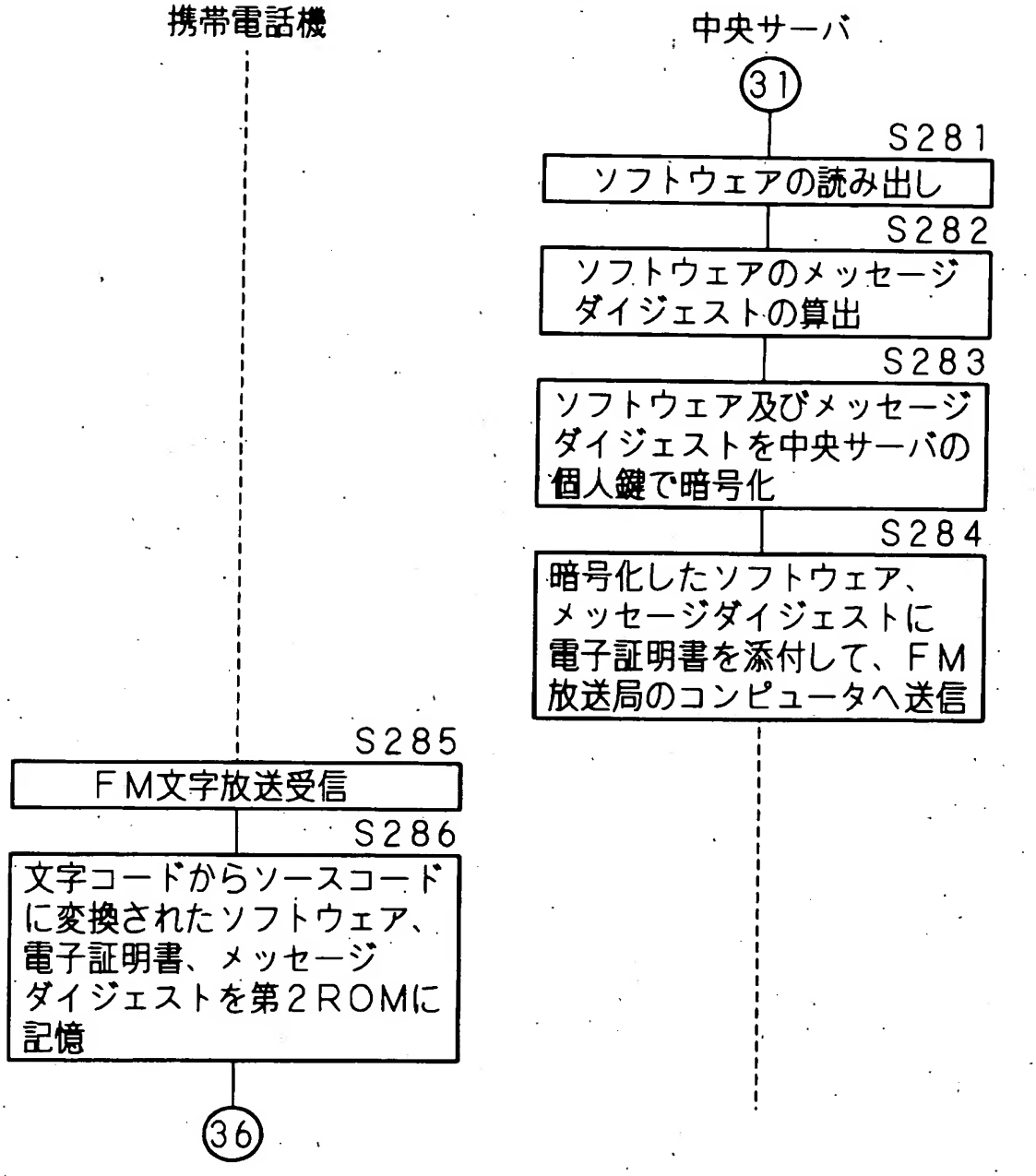
【図２７】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



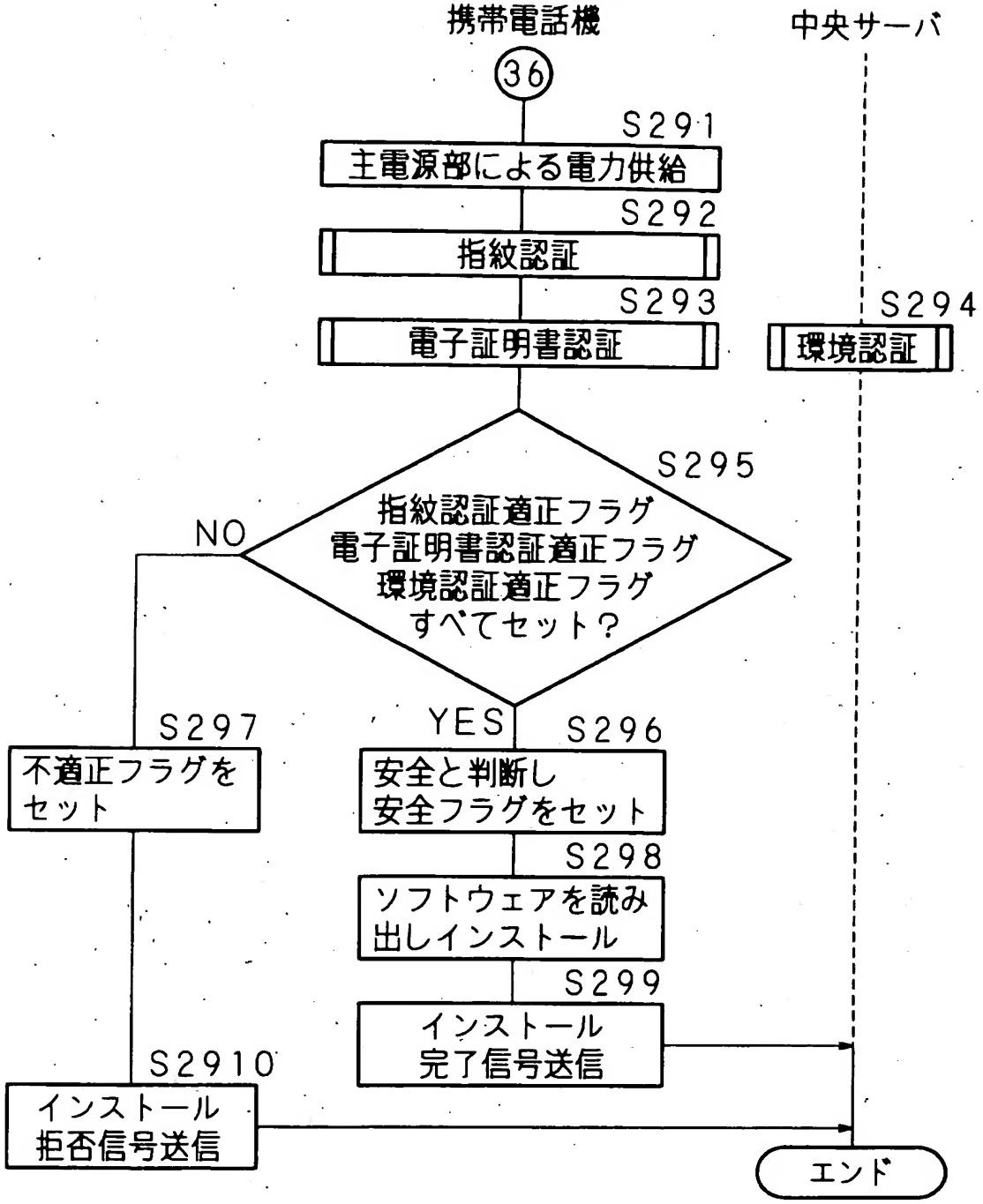
【図２８】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート



【図２９】

実施の形態４に係るソフトウェア提供処理の手順を示すフローチャート

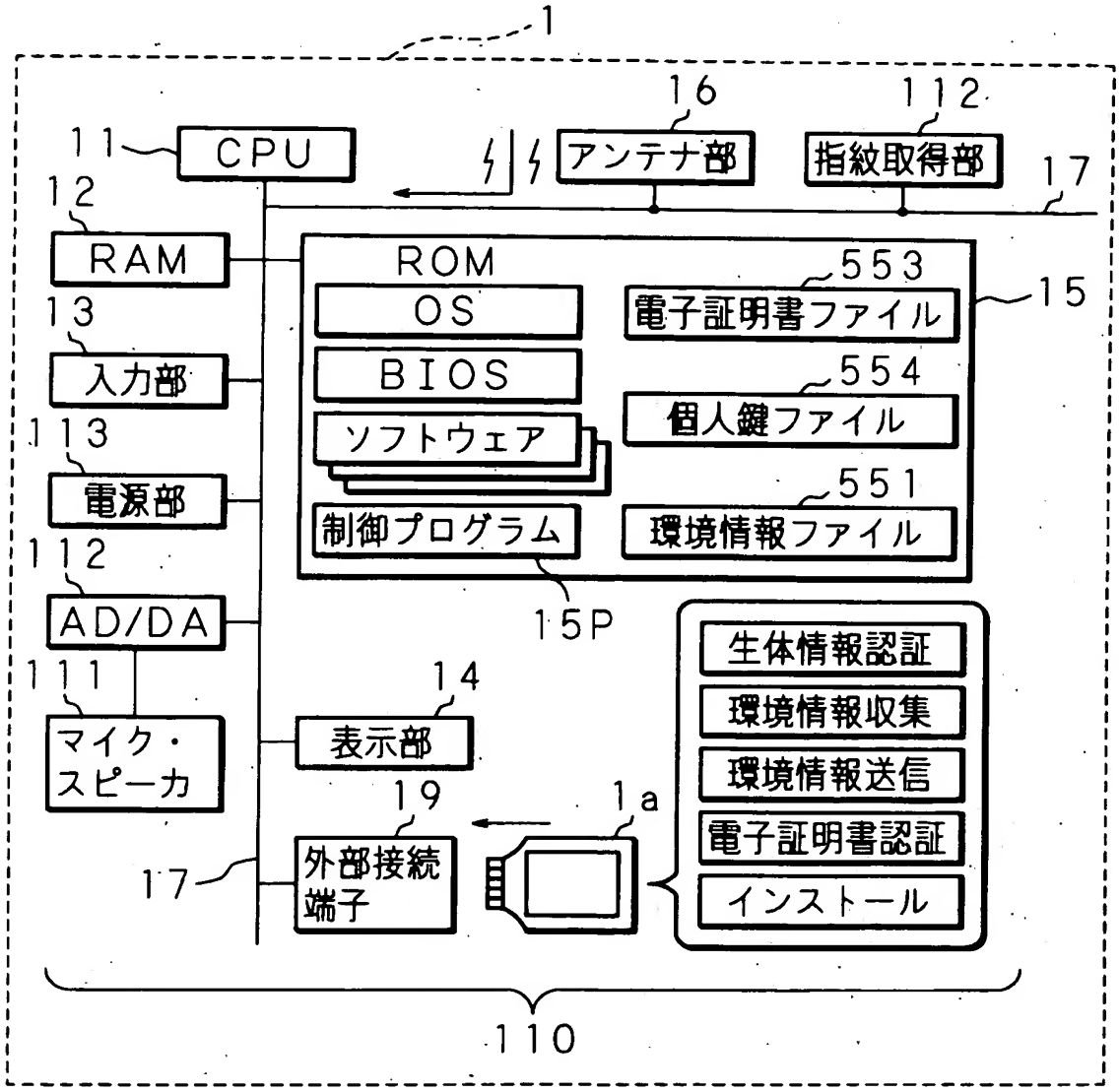


【図３０】

インストールされた消去用ソフトウェアの処理内容を示すフローチャート

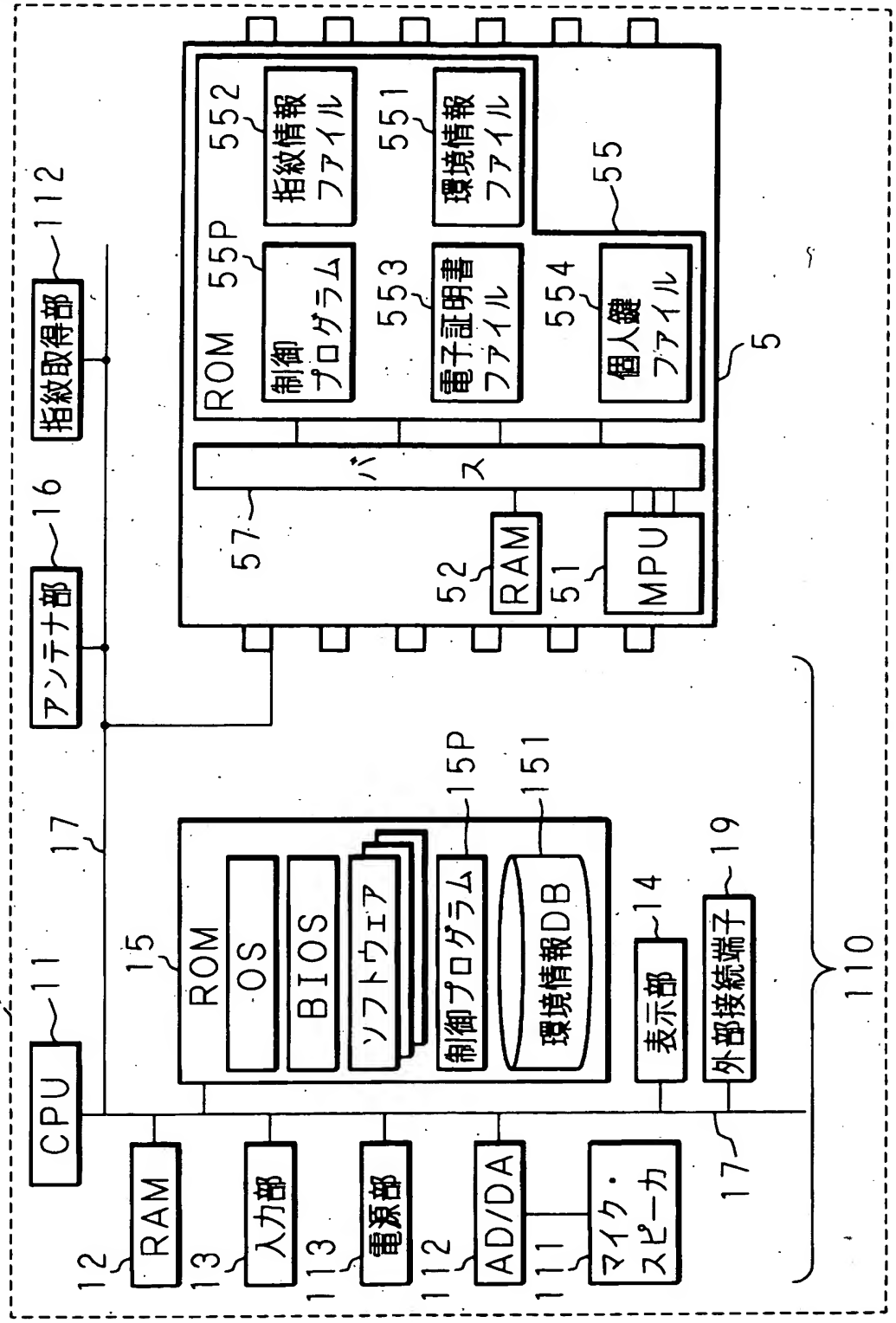
【図３１】

実施の形態５に係る携帯電話機のハードウェア構成を示すブロック図



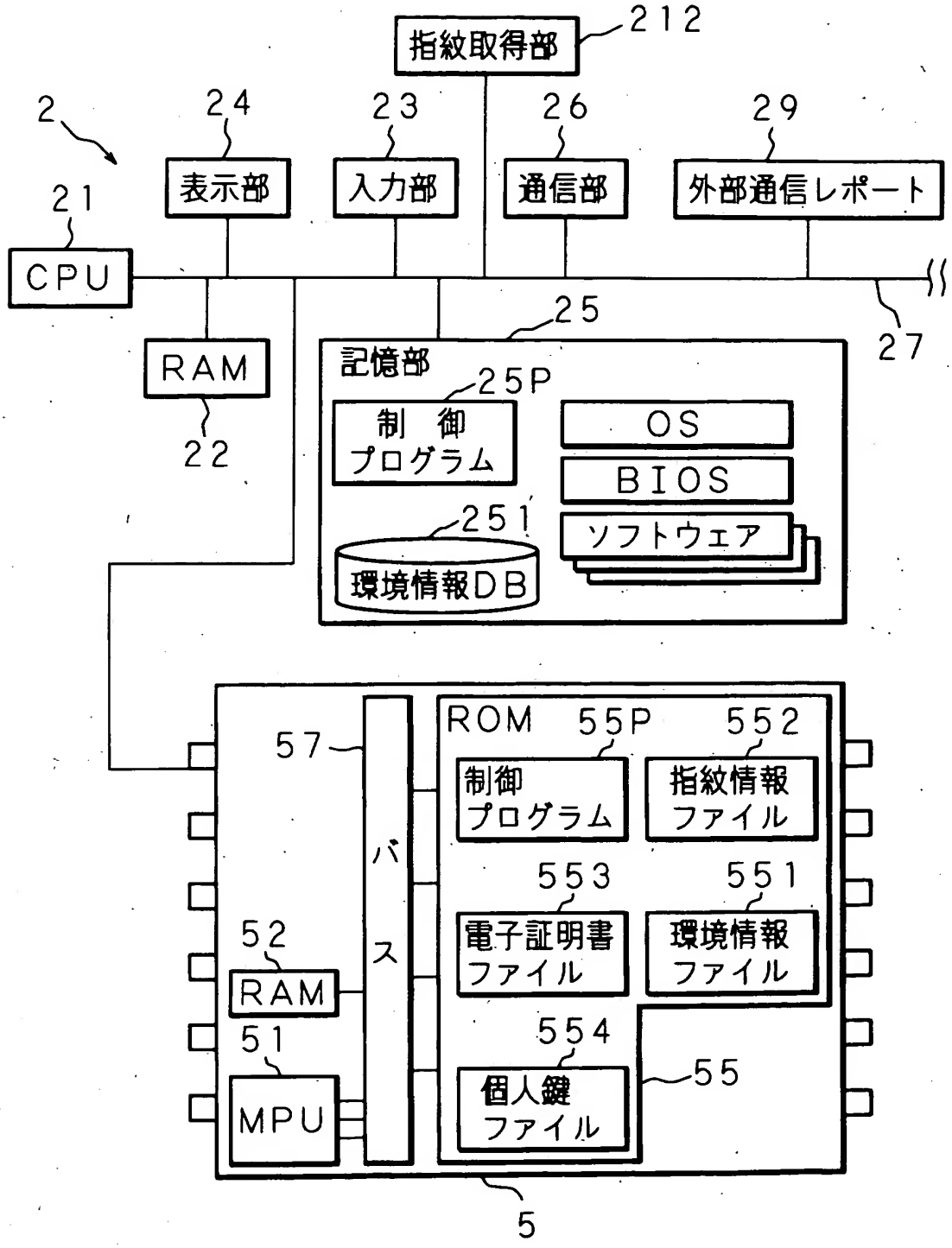
【図３２】

実施の形態６に係る携帯電話機のハードウェア構成を示すブロック図



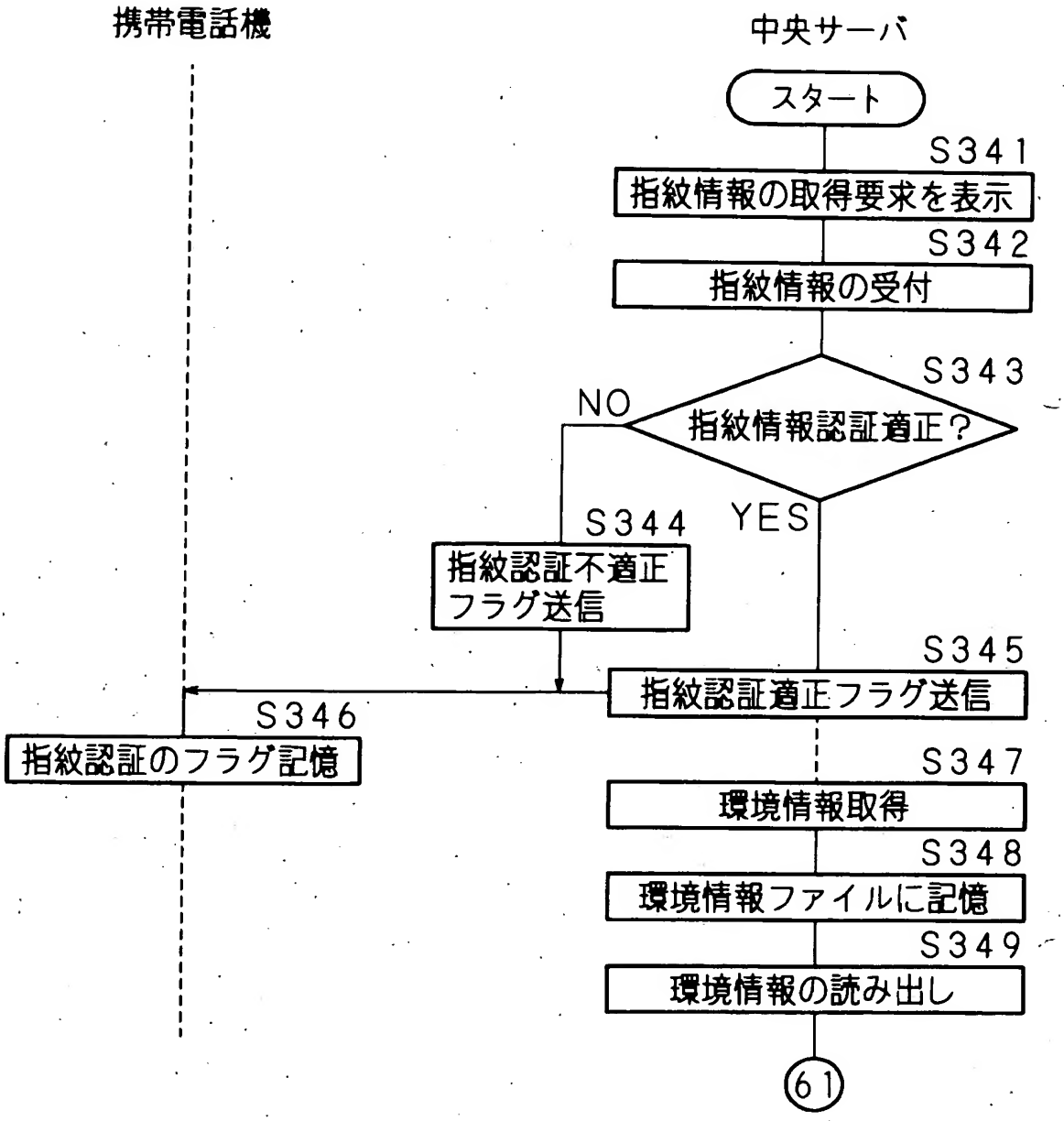
【図３３】

実施の形態６に係る中央サーバのハードウェア構成を示すブロック図



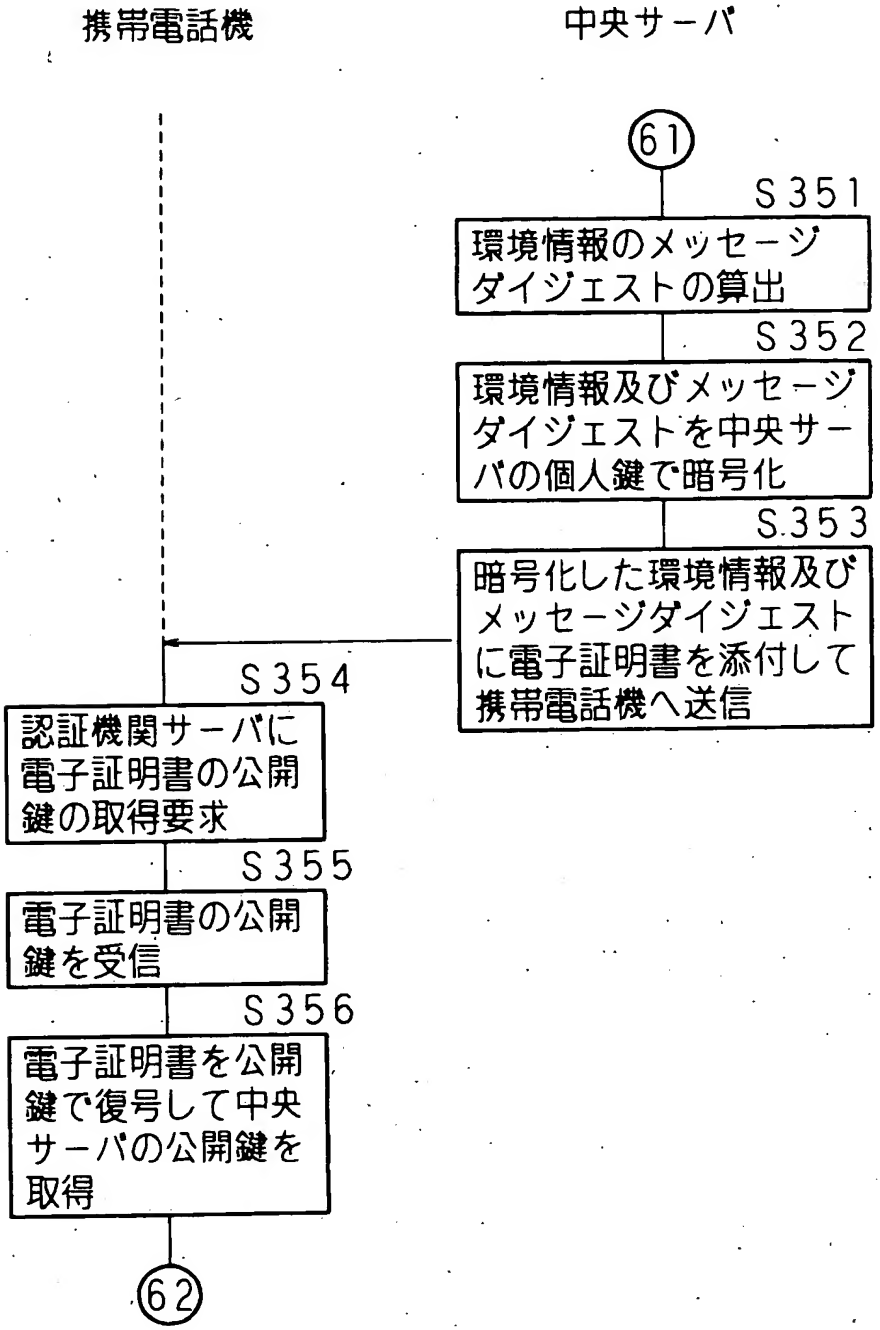
【図３４】

実施の形態６に係る認証処理の手順を示すフローチャート



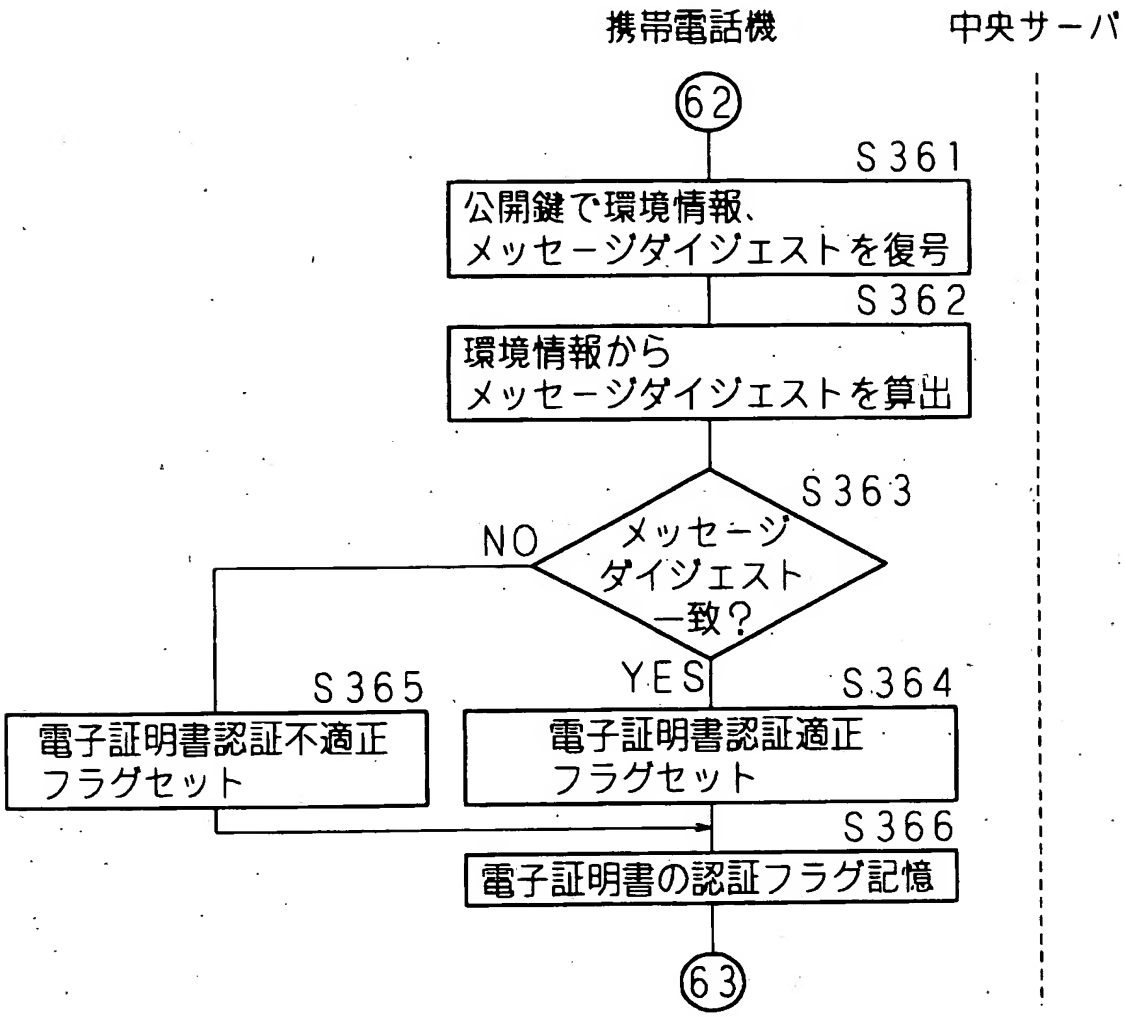
【図３５】

実施の形態６に係る認証処理の手順を示すフローチャート



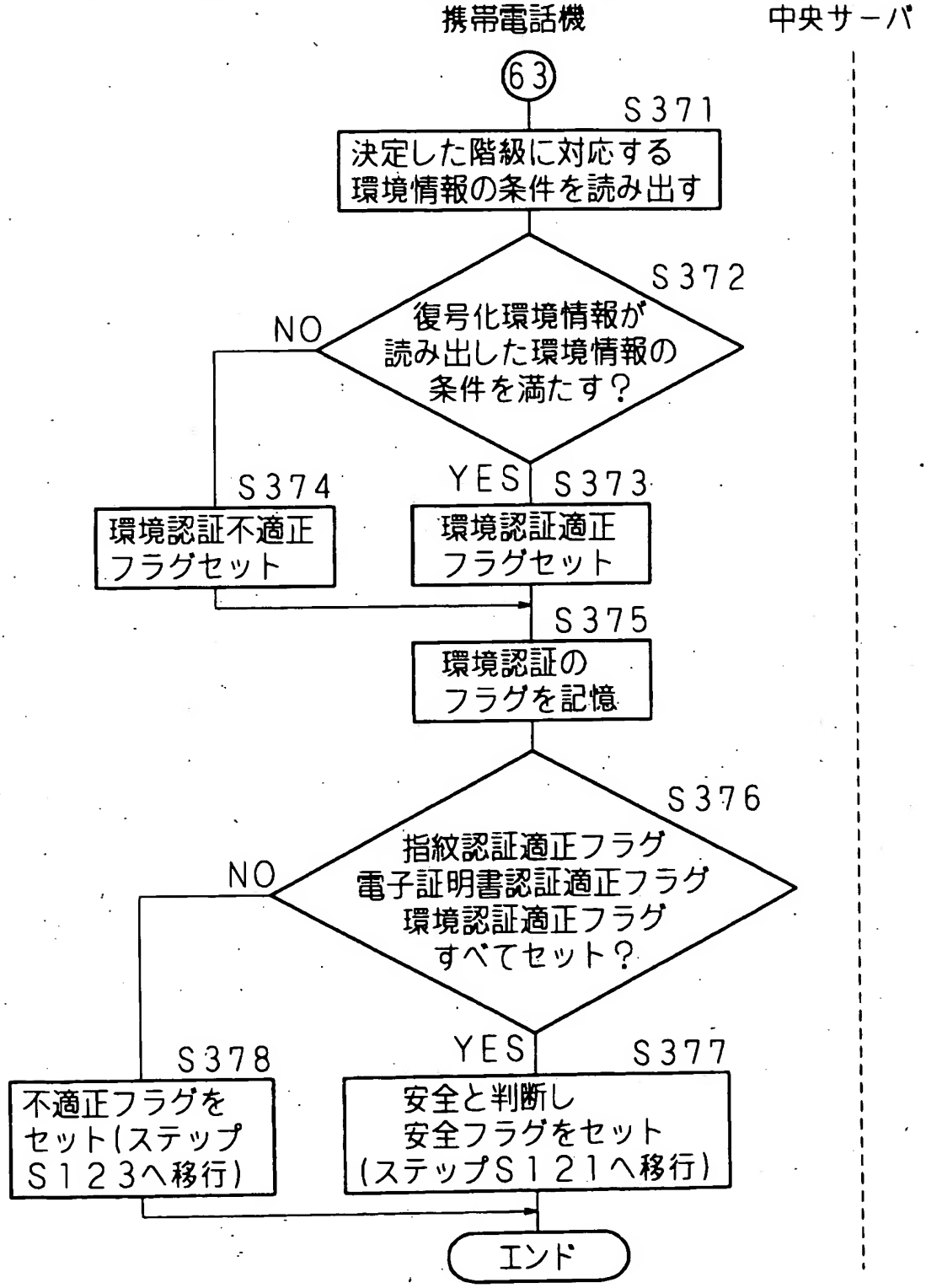
【図３６】

実施の形態６に係る認証処理の手順を示すフローチャート



【図３７】

実施の形態６に係る認証処理の手順を示すフローチャート



【書類名】　　要約書

【要約】

【課題】　安全性を高めることができ、また妥当な安全性を維持した上で円滑に情報の送受信を行うことが可能な安全性判断方法を提供する。

【解決手段】　生体情報認証を行い、また情報処理装置１の環境情報を収集する。情報処理装置１は収集した環境情報を第１認証装置２へ送信する。第２認証装置３から発行を受けた電子証明書及び個人鍵で暗号化された情報を第１認証装置２へ送信する。第１認証装置２は、第２認証装置３の公開鍵及び情報処理装置１の公開鍵を取得し、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する。第１認証装置２は環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置１を安全と判断する。

【選択図】　　図１

特願２００２－３２３２００

出願人履歴情報

識別番号　［０００００５２２３］

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　神奈川県川崎市中原区上小田中１０１５番地
氏　名　富士通株式会社

２．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社